ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΟΛΙΤΙΚΩΝ

ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΠΜΣ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΕΙΔΙΚΕΥΣΗ: ΔΙΕΘΝΕΣ ΟΙΚΟΝΟΜΙΚΟ,

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟ ΚΑΙ ΤΡΑΠΕΖΙΚΟ ΔΙΚΑΙΟ

**Διπλωματική εργασία**

**ΘΕΜΑ**

# «Ηλεκτρονικό οικονομικό έγκλημα: τυπολογίες και ρυθμιστική παρέμβαση για την αντιμετώπισή του σύμφωνα με τις διατάξεις του οικονομικού δικαίου».

Επιβλέπων: Αναπλ. Καθ. Χρ. Γκόρτσος

Επιμέλεια: **Σολανάκης Μιχάλης**

**Α.Μ. 1208Μ036**

Αθήνα, 2010

**Περιεχόμενα**

Πρώτο μέρος

*"Το χρήμα «έδειξεν ανθρώποις πανουργίας έχειν και παντός έργου δυσσέβειαν ειδέναι»*

*Σοφοκλής*

*Πρόσφατη έρευνα της WarRoom Research LLC κατέληξε στα εξής:*

*Η συντριπτική πλειοψηφία των εταιρειών που συμμετείχαν στην έρευνα είχαν υποστεί επίθεση στα συστήματά τους μέσα στο 2009. Περισσότερες από τις μισές εταιρείες δέχθηκαν πάνω από 30 επιθέσεις τους ελευταίους 12 μήνες. Σχεδόν το 60% είχαν οικονομικές απώλειες τουλάχιστον 200.000$ από κάθε επίθεση. Εσωτερικοί παράγοντες ήταν οι αιτία για το 75% των επιθέσεων στα πληροφοριακά συστήματα. Ο όρος «εσωτερικοί παράγοντες» θα λέγαμε πως σημαίνει «ανθρώπινος παράγων» στην ασφάλεια των πληροφοριών.*

*Οι περισσότερες επιχειρήσεις αρνούνται το γεγονός ότι έπεσαν θύμα ηλεκτρονικής επίθεσης και συγκαλύπτουν όλα τα στοιχεία, για να αποφύγουν πιθανό πλήγμα της αξιοπιστίας τους καθώς και ενδεχόμενες διοικητικές/ νομικές συνέπειες.*

# ΠΡΟΛΟΓΟΣ

Η καταλυτική παρουσία των νέων τεχνολογιών στην οικονομική ζωή άλλαξε άρδην τους παραδοσιακούς τρόπους εμπορίου και συναλλαγής με μετρητά. Ηλεκτρονικό εμπόριο, ηλεκτρονική μεταφορά κεφαλαίων, τηλεματική, κυβερνοχώρος είναι όροι τους οποίους συναντά κανείς σε καθημερινή βάση κατά τη διεκπεραίωση των οικονομικών και ιδιαίτερα των τραπεζικών συναλλαγών. Το μέλλον του εμπορίου και της παγκοσμιοποιημένης οικονομίας αποδεσμεύεται από τη φυσική παρουσία των συναλλασσομένων και την προσωπική επαφή των μερών και αναζητά νέες μεθόδους ταχείας και φθηνής συναλλαγής. Μαζί με την ευκολία του χρήστη - καταναλωτή προϊόντων και υπηρεσιών (χρηματοοικονομικών και μη) ο βασικότερος παράγοντας επιτυχίας της συναλλαγής χωρίς μετρητά, με αξιόγραφα ή μέσα της ηλεκτρονικής τραπεζικής, είναι η ασφάλεια των νέων μέσων πληρωμής.

Το ηλεκτρονικό έγκλημα αποτελεί μια από τις πιο σύγχρονες εκφάνσεις του οικονομικού εγκλήματος και η ραγδαία ανάπτυξη της τεχνολογίας τις τελευταίες δεκαετίες έχει καταστήσει την ανάγκη για αντιμετώπιση του επιτακτική. Κατά τη γνώμη του γράφοντος, το συγκεκριμένο ζήτημα έχει αποκτήσει ιδιαίτερη σημασία και ενδιαφέρον στις ημέρες μας ενώ η εκτενής εξέταση της ρυθμιστικής παρέμβασης από τους διεθνείς και κοινοτικούς νομοθέτες, που θα επιχειρηθεί, θα είναι σε θέση αναδείξει το σκεπτικό των προσπαθειών τους, το κατά πόσο έχει επιτευχθεί η αντιμετώπιση του προβλήματος, όπως και τα πιθανά κενά που υπάρχουν ακόμα και χρήζουν αποτελεσματικής επίλυσης.

Με την παρούσα διπλωματική εργασία θα γίνει μια προσπάθεια να παρουσιασθεί το θέμα του ηλεκτρονικού εγκλήματος ως μια από τις πτυχές του οικονομικού εγκλήματος. Τη σημερινή εποχή οπού η ανάπτυξη της τεχνολογίας πραγματοποιείται με ταχύτατους ρυθμούς, η άνοδος του δείκτη της ηλεκτρονικής εγκληματικότητας είναι εξίσου μεγάλη και οι οικονομικές απάτες που διαπράττονται έχουν οδηγήσει τους νομοθέτες στην λήψη μέτρων για την αντιμετώπιση του φαινομένου αυτού. Κατά συνέπεια, επίκεντρο της εν λόγω εργασίας θα αποτελέσει η ρυθμιστική παρέμβαση ως προς την αντιμετώπιση του ηλεκτρονικού οικονομικού εγκλήματος σύμφωνα με τις διατάξεις, κατά κύριο λόγο, του ευρωπαϊκού οικονομικού δικαίου καθώς και η επιρροή αυτού από το διεθνές κανονιστικό πλαίσιο.

Τα ζητήματα που θα εξετασθούν ειδικότερα θα είναι τα ακόλουθα:

Στην πρώτη ενότητα θα αναλυθούν οι έννοιες των όρων οικονομικό και ηλεκτρονικό έγκλημα, καθώς και οι τρόποι μέσω των οποίων συντελείται το ηλεκτρονικό οικονομικό έγκλημα ενώ παράλληλα θα παρουσιαστούν εκτενώς τα συστήματα πληρωμών και τα μέσα πληρωμών, γεγονός που θα διευκολύνει τον αναγνώστη ώστε να κατανοήσει την ουσία του προβλήματος και τη σπουδαιότητα της ρυθμιστικής παρέμβασης για την αποτελεσματική αντιμετώπισή του.

Στη δεύτερη ενότητα θα δοθεί ιδιαίτερη έμφαση στην «Απόφαση - πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών» . Η απόφαση αυτή αποτελεί μια από τις σημαντικότερες σε επίπεδο κοινοτικού οργάνου και συμπληρώνει το πλαίσιο ήδη ληφθέντων μέτρων για την καταπολέμηση κάθε μορφής απάτης που διαπράττεται με μέσα πληρωμών πλην των μετρητών. Ορίζει τις απατηλές συμπεριφορές οι οποίες ενδέχεται να συνιστούν ποινική παράβαση που υπόκειται σε κυρώσεις σε όλη την Ένωση, κυρώσεις οι οποίες πρέπει να είναι αποτελεσματικές, ανάλογες και αποτρεπτικές.

Παράλληλα θα γίνει επισκόπηση και ανάλυση του διεθνούς νομικού πλαισίου όπου κυρίαρχη θέση κατέχει η σύναψη της διεθνούς Σύμβασης στις 23 Νοεμβρίου 2001 στη Βουδαπέστη στο πλαίσιο του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο. Θεωρητικά οι Ευρωπαϊκές Κοινότητες και από το 1993 η Ευρωπαϊκή Ένωση δεν έχουν γνήσια ποινική νομοθετική εξουσία, δηλ. το δικαίωμα να θεσπίζουν ποινικούς κανόνες απευθυνόμενους στους πολίτες των κρατών μελών. Ωστόσο στην πράξη η ελλειπούσα αυτή εξουσία παρακάμπτεται με ευρωπαϊκές οδηγίες και αποφάσεις-πλαίσιο, οι οποίες υπαγορεύουν στον εθνικό νομοθέτη τους πρωτεύοντες, απαγορευτικούς ή επιτακτικούς, κανόνες δικαίου υποχρεώνοντας τον ταυτόχρονα να ποινικοποιήσει την παράβασή τους.

Οι αποφάσεις-πλαίσιο αποτελούν το βασικό νομοθετικό εργαλείο στο πλαίσιο του ενωσιακού (τρίτου) πυλώνα της ΕΕ για τη διαμόρφωση ενός «χώρου ελευθερίας, ασφάλειας και δικαιοσύνης» (άρθρο 2 παρ. 4 ΣυνθΕΕ). Σκοπός τους είναι η προσέγγιση των νομοθετικών και κανονιστικών διατάξεων των κρατών μελών (ά. 34 παρ. 2 β' ΣυνθΕΕ). Θεωρητικά υποδεικνύουν, όπως και οι οδηγίες, μόνο τον επιδιωκόμενο στόχο χωρίς να δεσμεύουν τα κράτη μέλη ως προς την επιλογή των μέσων. Ωστόσο στην πράξη οι αποφάσεις-πλαίσιο δεν περιορίζονται στην επιβολή απλής επιδίωξης στόχων, αλλά περιγράφουν (συνήθως κακότεχνα) αρκετά λεπτομερειακά συμπεριφορές, επιβάλλοντας

υποχρέωση των κρατών μελών να απειλήσουν κατ' αυτών κυρώσεις όχι απλώς αποτελεσματικές, ανάλογες και αποτρεπτικές, αλλά ποινικού χαρακτήρα. Οι αποφάσεις-πλαίσιο επικρίνονται συχνά λόγω του διοικητικού τους χαρακτήρα για δημοκρατικό έλλειμμα.

Στη συνέχεια θα επιχειρηθεί να εξετασθεί η συσχέτιση και επιρροή των διεθνών νομοθετημάτων και πρωτοβουλιών με το κοινοτικό αλλά και ελληνικό δίκαιο όπου το τελευταίο όπως θα δούμε παρουσιάζει πολύ μεγάλες ελλείψεις και χρήζει αναθεωρήσεως καθώς χαρακτηριστικά, ο όρος 'ηλεκτρονικό έγκλημα' δεν αναφέρεται πουθενά στο ελληνικό δίκαιο ενώ ισχύουν νόμοι εκδοθέντες ακόμα και αρκετές δεκαετίες πριν (π.χ Ν. 1805/1988 για τα εγκλήματα με Η/Υ).

Η έρευνα αυτή θα βοηθήσει εν τέλει στη διεξαγωγή χρήσιμων συμπερασμάτων για το κατά πόσο το υπάρχον νομικό πλαίσιο είναι αποτελεσματικό και έτοιμο να αντιμετωπίσει τις σύγχρονες αλλά και μελλοντικές προκλήσεις.

# Πρώτο μέρος

## 1. Εισαγωγή στο ηλεκτρονικό - οικονομικό έγκλημα

### 1.1. Η έννοια του οικονομικού εγκλήματος

Το οικονομικό έγκλημα αποτελεί μια κατηγορία του οργανωμένου εγκλήματος όπου η επίτευξη μεγάλου οικονομικού ή άλλου οφέλους μέσω διάπραξης παρανομιών είναι μία μόνο από τις δραστηριότητες που αναλαμβάνονται και ασφαλώς όχι ο αποκλειστικός στόχος των εμπλεκομένων σε αυτό[1]. Το έγκλημα, δηλαδή, αυτό έρχεται συνήθως ως απόρροια μιας ριψοκίνδυνης οικονομικής δραστηριότητας και όχι ως κύριος στόχος αυτής της δραστηριότητας. Οικονομικό έγκλημα, με την ευρύτερη του όρου έννοια, είναι αυτό που βλάπτει ή θέτει σε κίνδυνο τη λειτουργία της οικονομίας ή λειτουργικά σημαντικών κλάδων και θεσμών της[2]. Κυριαρχείται από το στοιχείο της απάτης, οι δε εκφραστές του είναι

---

[1] Για τον ορισμό ενός εγκλήματος ως οικονομικού Βλ. Β.Ζησιάδη, Η Οικονομική εγκληματικότητα, 2001, σελ 44 επ. κατά τον οποίο τρία είναι τα ασφαλή κριτήρια προκειμένου να χαρακτηριστεί ένα έγκλημα ως οικονομικό α) Η προσβολή του οικονομικού συστήματος β) Το μέγεθος της ζημίας το οποίο προκαλείται από τη συμπεριφορά του δράστη γ) η κατεύθυνση προς την οποία προκαλείται η ζημία.

Ειδικότερα, για να θεωρηθεί ένα έγκλημα ως οικονομικό θα πρέπει η ζημία την οποία προκαλεί το υποκείμενο να είναι μεγάλη προκειμένου να επέλθει βλάβη στο οικονομικό σύστημα. Δεν είναι όμως μόνο η ζημία η οποία έχει σημασία για το χαρακτηρισμό ενός εγκλήματος ως οικονομικού. Σημασία έχουν επίσης τα «τεχνάσματα» που χρησιμοποιεί ο οικονομικός εγκληματίας για να προκληθεί η ζημία και τα οποία κλονίζουν την εμπιστοσύνη του κοινού και των άλλων επιχειρήσεων στην αξιοπιστία του οικονομικού συστήματος, αν μάλιστα ληφθεί υπόψη ότι πολλές φορές, μια αιφνίδια άνοδος μιας επιχείρησης εξαιτίας οικονομικών εγκλημάτων, μπορεί να δημιουργήσει πρόσφορο έδαφος για τέλεση τέτοιων παράνομων πράξεων όταν υποψήφιοι δράστες διαβλέπουν δυνατότητες «επεμβάσεων» στο οικονομικό σύστημα λόγω αδυναμιών του και έλλειψης ασφαλιστικών δικλείδων. Το δεύτερο κριτήριο είναι η κατεύθυνση προς την οποία προκαλείται η ζημία. Το κατά πόσον δηλαδή ο υφιστάμενος τη ζημία διαδραματίζει σημαντικό ρόλο στο οικονομικό σύστημα του κράτους, όπως π.χ το Δημόσιο, οι τράπεζες, βιομηχανίες αλλά και ομάδες προσώπων, τα οποία επιδρούν στην οικονομική ζωή, όπως το καταναλωτικό κοινό. Η πρόκληση της ζημίας στην οικονομία μπορεί να είναι είτε άμεση, π.χ μεγάλης έκτασης φοροδιαφυγή από επιχείρηση είτε έμμεση, όταν π.χ η ζημία προκαλείται αρχικά σε μία επιχείρηση η οποία είναι ενταγμένη στο οικονομικό σύστημα, διαδραματίζοντας σημαντικό ρόλο στους κόλπους του και εν συνεχεία υφίσταται πλήγμα η οικονομία Σε κάθε περίπτωση πάντως η ζημία δεν θα πρέπει να περιορίζεται και να παραμένει μέσα στα πλαίσια της προσωπικής ζωής του θύματος αλλά να διοχετεύεται στο οικονομικό σύστημα στο οποίο εντάσσεται ο παθών. Χαρακτηριστικό είναι το παράδειγμα το οποίο χρησιμοποιεί ο Μανωλεδάκης (Η τυποποίηση των οικονομικών εγκλημάτων, σελ 266), σύμφωνα με το οποίο, μεμονωμένη απάτη μεγάλου οικονομικού μεγέθους, σε βάρος νεόπλουτου δήθεν φιλότεχνου, από έμπορο έργων τέχνης, με την εμφάνιση και πώληση ενός ζωγραφικού πίνακα ασήμαντης καλλιτεχνικής αξίας σαν έργο μεγάλου ζωγράφου, δεν συνιστά οικονομικό έγκλημα και τούτο διότι η περιουσιακή ζημία, έστω και μεγάλη, δεν έχει καμία σχέση με την καλή λειτουργία της οικονομίας. Τα εγκλήματα της σελίδας 20 του παρόντος ο *Ζησιάδης* τα εντάσσει σαφώς στην ως άνω κατηγορία.

[2] Συνεπώς, τα εγκλήματα των άρθρων 372 – 406 Π.Κ., δηλαδή τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, δεν αποτελούν σε κάθε περίπτωση οικονομικό έγκλημα. Με τον όρο αυτό επικράτησε να εννοούμε κάτι ειδικότερο. Νικόλαος Ανδρουλάκης, Γύρω από την οικονομική εγκληματικότητα, Δ' Συνέδριο, Ελληνική Εταιρία Ποινικού Δικαίου, Τα *οικονομικά εγκλήματα*, Εκδόσεις Σάκκουλα, Αθήνα, 1993, σελ. 9.

προικισμένοι με ιδιαίτερη και θαυμαστή οξύνοια και χρησιμοποιούν ευχερώς την, με ραγδαίους ρυθμούς, εξελισσόμενη ηλεκτρονική (δίκτυα υπολογιστών, διαδίκτυο) και λοιπή τεχνολογία.

Ως οικονομικό έγκλημα δεν πρέπει να θεωρείται κάθε πράξη που αποβλέπει σε περιουσιακό όφελος του δράστη ή τρίτου για λογαριασμό του οποίου ενεργεί τούτος. Επί παραδείγματι, η κλοπή δεν είναι οικονομικό έγκλημα εκ μόνου του λόγου ότι τελείται με σκοπό να αυξήσει την περιουσία[3] του ο δράστης κατά τρόπο αθέμιτο. Επίσης, δεν πρέπει να θεωρηθεί ως οικονομικό έγκλημα κάθε αξιόποινη πράξη που προκαλεί περιουσιακή βλάβη στο θύμα εκ μόνου του λόγου ότι επιφέρει αυτή τη βλάβη, ότι δηλαδή προσβάλλει περιουσιακό έννομο αγαθό, λ.χ. μια μεμονωμένη απάτη σε βάρος νεόπλουτου δήθεν φιλότεχνου από έμπορο έργων τέχνης, με την εμφάνιση και πώληση ενός ζωγραφικού πίνακα ασήμαντης καλλιτεχνικής αξίας σαν έργο μεγάλου ζωγράφου. Το οικονομικό μέγεθος, είτε ως προσβαλλόμενο έννομο αγαθό, είτε ως περιεχόμενο του σκοπού τέλεσης της αξιόποινης πράξης, δεν αρκεί από μόνο του για να προσδώσει στην πράξη αυτή τον χαρακτήρα (την ιδιότητα) του "οικονομικού εγκλήματος" υπό την τεχνική έννοια του όρου. Η ειδοποιός διαφορά του "οικονομικού εγκλήματος" υπό την τεχνική έννοια του όρου από το έγκλημα με οικονομικό απλώς περιεχόμενο ή με οικονομική απλώς σημασία έγκειται ακριβώς στην εμφάνισή του ως έκφρασης των μηχανισμών του οικονομικού συστήματος με κατάλληλο χειρισμό από το δράστη αυτών των μηχανισμών. Και οι συνέπειες της αξιόποινης πράξεις γίνονται αισθητές – σε μεγαλύτερη ή μικρότερη έκταση – ως εκτροπές (και προσβολές) του ίδιου του οικονομικού συστήματος. Το οικονομικό έγκλημα αποτελεί τελικά παθολογική απόρροια του οικονομικού συστήματος.

Οι αναφορές σε χώρες και νομικά πλαίσια του εξωτερικού που θα επιχειρηθεί στη συνέχεια, τόσο από τη θεωρητική όψη της φύσεως του οικονομικού εγκλήματος, όσο και από τη φαινομενολογική των εγκλημάτων που το διέπουν, κρίνεται αναπόφευκτη, καθώς, όπως

[3] Για την αναγκαιότητα να αποτελεί ένα υλικό αντικείμενο-ρυσιώδες στοιχείο του κοινωνικού χώρου, ώστε να τυποποιηθεί ως αξιόποινη η προσβολή του, βλ. *Μανωλεδάκη*, Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου, 1998,σελ.105 επ.

αποδεικνύεται από σχετικές έρευνες[4], η οικονομική εγκληματικότητα αποτελεί μια παγκόσμια υπόθεση.

## 1.2. Σύγχρονες μορφές οικονομικής εγκληματικότητας

### 1.2.1. Η έννοια του ηλεκτρονικού εγκλήματος

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μαζί όμως με τις αλλαγές αυτές που διευκολύνουν, προάγουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνίας, οι νέες τεχνολογίες και το Ίντερνετ διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα[5].

Σε μια προσπάθεια εννοιολογικού προσδιορισμού, θα λέγαμε ότι ως ηλεκτρονικό έγκλημα μπορεί να οριστεί: «*αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών*»[6], ενώ ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί «*κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη*

---

[4] Παγκόσμια Έρευνα του 2007 για το Οικονομικό Έγκλημα με τίτλο «Οικονομικό έγκλημα: Άνθρωποι, Κουλτούρα και Έλεγχοι» της Price waterhouse Coopers (PwC) σε συνεργασία με το Πανεπιστήμιο Martin-Luther, Halle- Wittenberg της Γερμανίας. [http://www.pwc.com/gr/eng/ins-sol/spec-nt/pr_crime161007_GR.pdf]

[5] Μεταξύ άλλων βλ. Αγγελής Ι. «*Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη*» (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp).

Ως *ηλεκτρονικό έγκλημα* μπορούμε επίσης να ορίσουμε το σύνολο των εγκλημάτων που σχετίζονται άμεσα με την κατάχρηση των δυνατοτήτων των Η/Υ. Ιωάννης Πανούσης, *Εγκληματολογία, Εγκληματολογική Έρευνα και ΜΜΕ*, Εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή 1999, σελ. 73. Βλ. επιπρόσθετα αναλυτικά σχετικά με το ηλεκτρονικό έγκλημα (τον ορισμό του, τις μορφές του κ.ό.κ.) Κ. Βλαχόπουλος, *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη, 2007. Επίσης, την ιστοσελίδα <www.e-crime.gr/news.htm>. Το ηλεκτρονικό έγκλημα υπολογίζεται ότι κοστίζει 70 δισ. ευρώ σε φθορές ή κλοπές ετησίως σε διεθνή κλίμακα. Για την Ελλάδα το μέγεθος αυτό αγγίζει τα 300 εκατομμύρια ευρώ. Κ. Τσαρούχας, Η μαφία του διαδικτύου, *Το Βήμα*, 21 Ιουλίου 2002, σελ. Α34

[6] Γιαννόπουλος Θ. (1986) «*Όψεις και Προβλήματα Ηλεκτρονικής Εγκληματικότητος*», Νομική Βιβλιοθήκη, σελ. 170επ, Forester, Tom and Morrison, Perry (1994) Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing. MIT Press

*επεξεργασία ή μετάδοση δεδομένων*»[7]. Σημειώνεται ότι ο ορισμός αυτός διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΟΣΑ, που συνεστήθη ειδικώς για να εξετάσει το θέμα της ηλεκτρονικής εγκληματικότητας. Ο ορισμός αυτός βέβαια είναι πολύ ευρύς και είναι ευνόητο ότι μόνο ως οδηγός μπορεί να χρησιμοποιηθεί. Η οριστικοποίησή του επαφίεται στον εθνικό νομοθέτη και στη νομολογία των δικαστηρίων.

### 1.2.2. Ιστορική εξέλιξη

Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα, σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων. Σήμερα, το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες, έχει πρόσβαση σε έναν Η/Υ, η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα μικρό παιδί μπορεί να χειρίζεται έναν προσωπικό υπολογιστή με ιδιαίτερη δεξιότητα.

Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος, επήλθε μετά την εμφάνιση των δικτύων. Τα δίκτυα, δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία, καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται. Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται, αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου. Σήμερα, οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία, τους τραπεζικούς μας λογαριασμούς, τις συνήθειές μας, τις προτιμήσεις μας κ.ά.

Το νέο περιβάλλον χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου[8], την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου, την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e – mail, chat,

---

[7] Μεταξύ άλλων, βλ. Μυλωνόπουλος Χρ. «*Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο*», Σειρά ΠΟΙΝΙΚΑ, Νο 33, σελ. 14, Λάζος, Γ. (2001). Πληροφορική & Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη, Τσουραμάνης, Χ. (2005). Ψηφιακή Εγκληματικότητα. Αθήνα: Κατσαρού Β.

[8] Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά (ΕΕ L 178, 17.7.2000, σ. 1).

newsgroups κ.λπ.), αλλά και την εξ αποστάσεως εκπαίδευση, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, την τηλεδιάσκεψη κ.ά.

### 1.2.3. Η οριοθέτηση της έννοιας του ηλεκτρονικού εγκλήματος

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί, όπως είδαμε, μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη , η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται *οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων* και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία[9].

Κρίνεται σκόπιμο και συνάμα αναγκαίο να επισημανθεί, ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δεν σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα. Για παράδειγμα, αποτελεί ηλεκτρονικό έγκλημα ο βιασμός μιας γυναίκας από έναν άνδρα, τον οποίο γνώρισε μέσω chat room στο Διαδίκτυο και ο χρόνος και τόπος συνάντησης, που διαπράχθηκε το έγκλημα, καθορίστηκε μέσω e-mail; Σαφώς, η απάντηση στο παραπάνω ερώτημα είναι αρνητική. Πρόκειται για ένα συμβατικό έγκλημα (το βιασμό), που διαπράχθηκε με τη βοήθεια των δυνατοτήτων επικοινωνίας που προσφέρει το Διαδίκτυο (chat και e-mail).

---

[9] Τσουραμάνης, Χ. Ψηφιακή Εγκληματικότητα. εκδ. Κατσαρού Β. Αθήνα, 2005

1.2.4. Αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων[10]

Οι επιθέσεις μεγάλης κλίμακας που στρέφονται εναντίον συστημάτων πληροφοριών ή οργανισμών και ατόμων (συχνά μέσω των επονομαζόμενων «δικτύων προγραμμάτων ρομπότ» (botnets) φαίνεται ότι εμφανίζονται με συνεχώς αυξανόμενη συχνότητα. Επίσης, έχουν σημειωθεί προσφάτως περιστατικά συστηματικών, καλά συντονισμένων και ευρείας κλίμακας άμεσων επιθέσεων κατά των κρίσιμων υποδομών πληροφόρησης ενός κράτους. Το φαινόμενο αυτό έχει επιδεινωθεί εξαιτίας της συγχώνευσης των τεχνολογιών και της επιταχυνόμενης διασύνδεσης των συστημάτων πληροφοριών, στις οποίες οφείλεται το γεγονός ότι τα συστήματα αυτά έχουν γίνει πιο ευάλωτα. Οι επιθέσεις αυτές είναι συχνά καλά οργανωμένες και χρησιμοποιούνται για σκοπούς εκβιαστικής απόσπασης. Μπορούμε να υποθέσουμε ότι τα κρούσματα αυτά παρουσιάζονται έτσι ώστε να μετριάζεται η σοβαρότητά τους, πράγμα που οφείλεται εν μέρει στο ενδεχόμενο ζημιών των εμπορικών συμφερόντων των εμπλεκόμενων επιχειρήσεων σε περίπτωση που θα δινόταν δημοσιότητα σε προβλήματα ασφάλειας.

Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου. Στη συνθήκη της Βουδαπέστης του Συμβουλίου της Ευρώπης[11] γίνεται λόγος για κυβερνοέγκλημα ή έγκλημα στον κυβερνοχώρο (cyber crime), ενώ η απόφαση-πλαίσιο 2005/222/ΔΕΥ[12] της ΕΕ αναφέρεται μόνο στις «επιθέσεις κατά των συστημάτων πληροφοριών»

Θα μπορούσαμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

• μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών,

• μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές,

• μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ' οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

---

[10] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Επιτροπή των περιφερειών, Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, Βρυξέλλες, 22.5.2007 COM(2007) 267 τελικό

[11] *Σύμβαση του Συμβουλίου της Ευρώπης αριθμ. 185* (Βουδαπέστη 23/11/2001)

[12] Δημοσιεύθηκε στην εφημερίδα της ΕΕ L 69 16/3/2005, σελ. 67

Πρέπει να αναφέρουμε πως βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notebook κ.λπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί σύμφωνα με τον Shinder[13]:

• να αποτελεί τον στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.

• να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).

• να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

### 1.2.5. Το ζήτημα σχετικά με την ορολογία

Πρόβλημα παράλληλα δημιουργείται όσον αφορά στην ελληνική νομική ορολογία, γιατί κατά κανόνα τόσο η τεχνική όσο και η νομική ορολογία είναι διατυπωμένη στα αγγλικά με αποτέλεσμα η αντίστοιχη μεταφορά των όρων αυτών στα ελληνικά να μην είναι ούτε εύκολη ούτε δόκιμη.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλλουν: e-crime, cybercrime, computer-crime, internet related crime και hitech-crime είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer-crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στη δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

[13] Κ. Βλαχόπουλος, *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα, 2007

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, ψηφιακό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

1.2.6. Μορφές του ηλεκτρονικού εγκλήματος

Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται[14]. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime)[15], του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001.

Στη συνθήκη της Βουδαπέστης, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα και η οποία θα εξετασθεί εκτενώς παρακάτω, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.

3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.

4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της

[14] http://www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=90

[15] βλ. και Αγγέλη Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), ΠοινΔικ 2001, σ. 1218 επ.

αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά.[1] Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση.

### 1.2.7. Κατηγορίες δραστών ηλεκτρονικών εγκλημάτων

Τους εγκληματίες του κυβερνοχώρου θα μπορούσαμε να τους διακρίνουμε σε δυο βασικές κατηγορίες[16] :

• σ΄ αυτούς που "επιτίθενται" (εισβάλουν) στους ηλεκτρονικούς υπολογιστές απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη "εισβάλουν " σε υπολογιστή δια της χρήσεως του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία,

• σ΄ αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη ανήκουν αυτοί που δεν " εισβάλουν " απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν ( π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμό τους. Σύμφωνα με Anderson[17], υπάρχουν οι εξής κατηγορίες δραστών ηλεκτρονικών εγκλημάτων:

- Εξωτερικοί δράστες: Πρόσωπα προερχόμενα από τον εξωτερικό χώρο της επιχείρησης – στόχου τους, που πετυχαίνουν πρόσβαση στο σύστημα της δίχως να έχουν εξουσιοδότηση. Αυτή είναι η κατηγορία η οποία ανταποκρίνεται περισσότερο στην παραδοσιακή εικόνα του χάκερ – δεν έχουν νόμιμο σκοπό και ως εκ τούτου δεν έχουν ρόλο να παίξουν στο σύστημα.
- Εσωτερικοί δράστες: χρήστες του συστήματος, που έχουν εξουσιοδότηση και αποκτούν πρόσβαση σε δεδομένα, πηγές ή προγράμματα δίχως να έχουν τέτοιο δικαίωμα. Οι υποκατηγορίες τους έχουν ως εξής: *Μεταμφιεσμένοι*: χρήστες, που δρουν χρησιμοποιώντας την ταυτότητα άλλου χρήστη. *Κρυφοί χρήστες*: χρήστες, που επιτυγχάνουν παράνομη πρόσβαση σε αρχεία με σκοπό τον έλεγχο και την εξέταση του περιεχομένου τους. *Έκπτωτοι*:

---

[16] Furnell, S.. Κυβερνοέγκλημα. Αθήνα: Παπαζήση, 2006

[17] Anderson R. «*Security Engineering: A guide to building dependable distributed systems*», New York: John Wiley and Sons, Inc, 2001

χρήστες, που έχουν την άδεια να χρησιμοποιούν το σύστημα και τις πηγές του στις οποίες αποκτούν πρόσβαση, αλλά έχουν απολέσει τα προνόμιά τους. Αυτή η ομάδα είναι τυπικά η πιο δύσκολα αναγνωρίσιμη, επειδή τα πρόσωπα έχουν νόμιμη πρόσβαση στο σύστημα και γνωρίζουν πώς να το χρησιμοποιούν.

### 1.2.8. Διαφορές ηλεκτρονικών εγκλημάτων από τα παραδοσιακά οικονομικά εγκλήματα

Οι διαφορές των ηλεκτρονικών εγκλημάτων από τα παραδοσιακά εγκλήματα, μπορούν να εντοπιστούν στα εξής χαρακτηριστικά:

• Διαπράττονται συνήθως από μακρινή απόσταση,

• Ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος,

• Αποδίδουν μεγάλα κέρδη, με μικρό κίνδυνο ανακάλυψης του δράστη τους,

• Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος,

• Οι οικονομικές απώλειες, που προξενούνται στα «ψηφιακά» θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων και

• Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμία επίσημη αρχή, δηλαδή ο «σκοτεινός αριθμός» τους είναι ιδιαίτερα σημαντικός

Τα ηλεκτρονικά εγκλήματα όπως μπορεί εύκολα κάποιος να αντιληφθεί είναι ιδιαίτερα σημαντικά και ενδέχεται να προκαλέσουν πολύ μεγαλύτερες ζημίες από τα υπόλοιπα «κοινά» οικονομικά εγκλήματα. Θα μπορούσαμε να επισημάνουμε ενδεικτικά τα εξής για να τεκμηριώσουμε την πρότασή αυτή:

• Οι οικονομικές απώλειες από αυτά είναι πολύ μεγαλύτερες, όπως συνήθως διαπιστώνεται.

• Η ανακάλυψη των ενόχων και η προσαγωγή τους στη δικαιοσύνη συναντάει μεγαλύτερες δυσκολίες απ' ότι στα κοινά εγκλήματα,

• Οι ψηφιακοί εγκληματίες δεν έχουν φυσική παρουσία στον τόπο του εγκλήματος - σε αντίθεση με τους κοινούς εγκληματίες -, πράγμα που καθιστά δυσκολότερο τον εντοπισμό και τη σύλληψή τους και

• Οι πληροφορίες που υποκλέπτονται από μια επιχείρηση[18] είναι δυνατό να είναι τόσο κρίσιμες γι' αυτή που μπορεί να οδηγήσουν στην απώλεια της εμπορικής της πίστης και σε κάποιες περιπτώσεις ακόμα και στη χρεωκοπία της με ότι αυτό συνεπάγεται για τους εργαζόμενους σε αυτή. Κάτι τέτοιο είναι μάλλον αδιανόητο να συμβεί σε περίπτωση που γίνει κάποιο κοινό έγκλημα (π.χ. διάρρηξη, ληστεία) σε βάρος της.

## 1.3. Η ηλεκτρονική οικονομική εγκληματικότητα

### 1.3.1. Ιδιαίτερα γνωρίσματα των ηλεκτρονικών οικονομικών εγκλημάτων

Ο κύριος όγκος των ηλεκτρονικών εγκλημάτων εντάσσεται στη κατηγορία των οικονομικών ηλεκτρονικών εγκλημάτων. Τα ηλεκτρονικά οικονομικά εγκλήματα απαρτίζουν τον κύριο όγκο των διαπιστωμένων ηλεκτρονικών εγκλημάτων και επίσης είναι τα εγκλήματα που τραβούν την προσοχή των ερευνητών. Παρά το γεγονός ότι πολλές αξιόποινες συμπεριφορές φαίνεται να πλήττουν, κυρίως ή αποκλειστικά, έννομα αγαθά (π.χ. απόρρητο επικοινωνιών, υπομνήματα, ανηλίκους[19]), δεν είναι υπερβολικό να λεχθεί ότι τα οικονομικά εγκλήματα συνιστούν τον πυρήνα των ηλεκτρονικών εγκλημάτων[20]. Η σύνδεση των υπολογιστών στο Διαδίκτυο έχει οδηγήσει μάλιστα στη θέση ότι η αθέμιτη πρόσβαση σε δεδομένα (hacking) έχει αναχθεί σε ένα είδος «βασικού εγκλήματος»[21], το οποίο τελείται συχνά προκειμένου να τελεσθεί κάποιο οικονομικό έγκλημα

• Τα ηλεκτρονικά οικονομικά εγκλήματα γίνονται αντιληπτά από τους ενδιαφερόμενους σε σχετικά μικρό χρονικό διάστημα μετά την τέλεσή τους.

---

[18] Βλ. παρακάτω «Η οικονομική κατασκοπεία», σελ.21

[19] Στην περίπτωση της πορνογραφίας ανηλίκων του άρθρου 348 Α ΠΚ πρόκειται για έγκλημα οικονομικής εκμετάλλευσης της γενετήσιας ζωής, αφού ο Έλληνας νομοθέτης, αντίθετα με άλλες εθνικές νομοθεσίες και την Σύμβαση του Συμβουλίου της Ευρώπης, απαιτεί ο αυτουργός του εγκλήματος να ενεργεί από κερδοσκοπία

[20] U.Sieber σε T.Hoeren, U.Sieber (Hsg.), Handbuch Multimedia Recht, 1999, κεφ.19, αριθμ. 29

[21] U.Sieber, ό.π.. Στην ίδια κατεύθυνση και ο Ν. Κουράκης, Το οικονομικό έγκλημα στην Ελλάδα σήμερα σε: του ιδίου Εγκληματολογικοί ορίζοντες Β΄, 2005 σελ.185-187. που εντοπίζει επτά περιπτώσεις παραβίασης δεδομένων (hacking) που σχετίζονται με το οικονομικό έγκλημα ( φθορά προγραμμάτων, δυσφήμηση-παράνομη συγκριτική διαφήμιση, βιομηχανική κατασκοπία, ηλεκτρονική κλοπή πιστωτικών καρτών, ηλεκτρονική κλοπή τραπεζικών κωδικών, ηλεκτρονική απάτη σε χρηματιστηριακές συναλλαγές)

• Είναι μετρήσιμα με μεγάλη ακρίβεια – τουλάχιστον όσον αφορά στα άμεσα οικονομικά του μεγέθη.

• Τραβούν το ενδιαφέρον μεγάλων επιχειρήσεων, οι οποίες έχουν διαθέσει πολύ σημαντικούς πόρους για την διερεύνηση τους.

### 1.3.2. Κατηγοριοποιήσεις ηλεκτρονικών οικονομικών εγκλημάτων

Η συχνότητα και η σημασία του ηλεκτρονικού οικονομικού εγκλήματος έχουν θεωρηθεί επαρκείς λόγοι για την δημιουργία συστηματικών κατηγοριοποιήσεων του[22]. Σημαντικοί επιστήμονες του χώρου, όπως ο Wasik[23] και ο Sieber[24], έχουν και εκείνοι προχωρήσει σε κατηγοριοποιήσεις του ηλεκτρονικού οικονομικού εγκλήματος, ανάλογα με τα εμπειρικά δεδομένα που ο καθένας είχε στην διάθεσή του.

- Κατηγοριοποίηση του Sieber[25] : οικονομικά εγκλήματα σχετιζόμενα με

υπολογιστές:

1. απάτη ηλεκτρονικής παραποίησης ενάντια σε συστήματα επεξεργασίας δεδομένων
2. ηλεκτρονική κατασκοπεία και κλοπή λογισμικού
3. ηλεκτρονική δολιοφθορά
4. κλοπή υπηρεσιών
5. μη εξουσιοδοτημένη πρόσβαση σε συστήματα επεξεργασίας δεδομένων
6. παραδοσιακά οικονομικά αδικήματα με την χρήση επεξεργασίας δεδομένων.

(Γερμανία, 1986)

- Κατηγοριοποίηση του Wasik[26]: απάτες και ηλεκτρονικές κλοπές:

---

[22] Για τις διακρίσεις των εγκλημάτων του κυβερνοχώρου βλ. και *Ι. Αγγελής,* Διαδίκτυο και ποινικό δίκαιο, Έγκλημα στον κυβερνοχώρο, Ποιν.Χρον Ν΄, 675 επ.

[23] http://www.johnwasik.com/

[24] http://de.wikipedia.org/wiki/Ulrich_Sieber

[25] Λάζος, Γ. (2001). Πληροφορική & Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη.

[26] Λάζος, Γ.. Πληροφορική & Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη. 2001

1. παραπλάνηση

2. κλοπή

3. ψευδή λογιστικά και πλαστογραφία

4. συνωμοσία για εξαπάτηση

5. μη εξουσιοδοτημένη αφαίρεση πληροφοριών

6. εμπορικά μυστικά

7. δικαιώματα αντιγραφής.

(Μ. Βρετανία, 1991)

Ήδη κατά την πενταετία, που ακολούθησε μεταξύ των παραπάνω δημοσιεύσεων το Hacking αυτονομήθηκε ως κατηγορία ηλεκτρονικού εγκλήματος. Επίσης η κατηγορία της ηλεκτρονικής δολιοφθοράς διερευνήθηκε και δεν περιορίζεται στο οικονομικό στοιχείο.

### 1.3.3. Η δυσκολία συλλογής στατιστικών στοιχείων

Τα στατιστικά στοιχεία που διαθέτουμε για το ηλεκτρονικό έγκλημα και προέρχονται από τις διωκτικές αρχές, δεν μπορούν να χαρακτηριστούν αξιόπιστα. Υπάρχουν δύο βασικά εμπόδια[27] που δεν μας επιτρέπουν να έχουμε ακριβή στοιχεία σύμφωνα με τον Kabay[28]:

Η δυσκολία εντοπισμού του ηλεκτρονικού εγκλήματος: Το πρόβλημα της λεγόμενης «κρυφής» εγκληματικότητας, που το συναντάμε σε όλες τις μορφές εγκλημάτων, παρουσιάζει μεγάλη συχνότητα στην περίπτωση των ηλεκτρονικών εγκλημάτων. Ο όρος αναφέρεται σε εγκλήματα που έχουν τελεσθεί, χωρίς να το έχουν αντιληφθεί τα θύματα.

Η διστακτικότητα αναφοράς από τα θύματα: Ακόμη και αν το θύμα αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, διστάζει να την αναφέρει στις διωκτικές αρχές, με αποτέλεσμα, να μην είναι δυνατή η συστηματική συλλογή στατιστικών στοιχείων. Οι λόγοι για τη μη αναφορά των ηλεκτρονικών εγκλημάτων ποικίλλουν με κυρίαρχο το φόβο της

---

[27] Κ. Βλαχόπουλος, *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα, 2007

[28] http://www.mekabay.com/

εταιρείας, που δέχθηκε την επίθεση, ότι αν αποκαλυφθεί το γεγονός θα έχει αρνητικές συνέπειες στην εικόνα της προς τους πελάτες της.

Εκτιμάται ότι τα στατιστικά στοιχεία που διαθέτουμε από τις διωκτικές αρχές, αντιπροσωπεύουν μόνο το 10% της πραγματικής έκτασης του φαινομένου. Για το λόγο αυτό, η μέτρηση του ηλεκτρονικού εγκλήματος, γίνεται με εναλλακτικές μεθόδους, όπως συνεντεύξεις και έρευνες σε συγκεκριμένες κατηγορίες ατόμων

## 1.4. Μέθοδοι τέλεσης ηλεκτρονικών οικονομικών εγκλημάτων.

### 1.4.1. Η απάτη μέσω του διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης[29] αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του.[30] Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών, η οποία και θα αποτελέσει κύριο αντικείμενο μελέτης στη δεύτερη ενότητα της παρούσας εργασίας.

Αντίστοιχες περιπτώσεις εγκληματικής συμπεριφοράς καλύπτουν και οι συχνά χρησιμοποιούμενοι όροι hacking[31] (παρέμβαση), phishing[32] («ψάρεμα»), pharming[33] («καλλιέργεια»), ID theft[34] (κλοπή ταυτότητας), spamming[35] κ.λπ.

---

[29] Βλ. Αρ. 386 ΠΚ

[30] Βλ. Αρ. 386Α ΠΚ.

[31] Το *Hacking* αποτελεί η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικών υπολογιστών η οποία καταρχήν δεν γίνεται με σκοπό την δολιοφθορά ή την καταστροφή, αλλά για την ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας. Βλ. επιπλέον σχετικά R. Doswell & G. Simons, *Πληροφορική και Εγκληματικότητα*, Εκδόσεις Δαυλός, Αθήνα 1990, σελ. 69 – 90.

[32] Όπως το ίδιο το όνομά του υπονοεί -παραλλαγή του αγγλικού «fishing» (ψάρεμα), το **Phishing** αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα. Βλ. http://en.wikipedia.org/wiki/Phishing

Στον αγγλοσαξονικό χώρο, και όχι μόνον, όλες οι περιπτώσεις ηλεκτρονικής απάτης που συνδυάζονται με απόκτηση στοιχείων που επιτρέπουν στον δράστη να διενεργεί συναλλαγές επ' ονόματι άλλου (του θύματος) ονομάζονται κλοπή ταυτότητας (ID theft) και αποτελούν πλέον σημαντικότατο τμήμα οικονομικού ηλεκτρονικού εγκλήματος με μεγάλο σκοτεινό αριθμό, καθώς οι τράπεζες και άλλοι μεγάλοι οργανισμοί αποφεύγουν να δημοσιοποιούν στοιχεία, που αποδεικνύουν τις αδυναμίες των συστημάτων και μπορούν να δημιουργήσουν ανασφάλεια στους πελάτες τους.

Η ένταξη πολλών περιπτώσεων ηλεκτρονικής απάτης στο χώρο του διαδικτυακού εγκλήματος έφερε στο προσκήνιο και μια άλλη κατηγορία προσώπων που εντάσσονται στο κύκλωμα, ως ενδιάμεσοι μεταξύ θύματος και δράστη. Ο δράστης του phishing[36] και του pharming, αφού εξασφαλίσει τους αριθμούς αναγνώρισης και άλλα στοιχεία του λογαριασμού του θύματος επιχειρεί να αποκομίσει περιουσιακό όφελος, χωρίς όμως να γίνει αντιληπτός από τις αρχές[37]. Συχνά, λοιπόν, χρησιμοποιεί τρίτα πρόσωπα, τους αποκαλούμενους οικονομικούς διαχειριστές (finance managers), με τους οποίους συνάπτει την εξής συμφωνία: Χρησιμοποιώντας τα στοιχεία του θύματος εμβάζει χρηματικό ποσό στο λογαριασμό του οικονομικού διαχειριστή, ο οποίος αφαιρεί ένα ποσοστό ως προμήθεια και μεταβιβάζει το υπόλοιπο στον δράστη μέσω υπηρεσιών διεθνούς διαβίβασης χρημάτων. Έτσι, ο μεν

---

[33] "Pharming" σημαίνει ότι εγκληματίες χάκερ ανακατευθύνουν την κίνηση του Internet από μία τοποθεσία Web σε μια άλλη, πανομοιότυπη έτσι ώστε να ξεγελάσουν τον χρήστη και να καταχωρίσει το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής τοποθεσίας. Το pharming πιθανόν να θυμίζει τις απάτες ηλεκτρονικού "ψαρέματος" με μηνύματα ηλεκτρονικού ταχυδρομείου, όμως το pharming είναι πιο ύπουλο, αφού ο χρήστης μπορεί να κατευθυνθεί σε μία πλαστή τοποθεσία χωρίς τη συμμετοχή του και χωρίς να το γνωρίζει. Βλ. http://en.wikipedia.org/wiki/Pharming

[34] Για τις μεθόδους της κλοπής ταυτότητας βλ. αναλυτικά *A.M. Marshall & B.C. Tompsett, Identity theft in an online world*, Computer law & security report , 2005, 128 επ.

[35] Δηλαδή η μέθοδος αποστολής διαφημιστικών μηνυμάτων μέσω e – mail, χωρίς να έχει προηγηθεί αίτημα του παραλήπτη και πολύ περισσότερο χωρίς τη συναίνεσή του. Βλ. Ελίζα Αλεξανδρίδου, *Το δίκαιο του ηλεκτρονικού εμπορίου*, Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη 2004, σελ. 195 επ.

[36] Οι πρώτες προσπάθειες phishing είχαν λίγες πιθανότητες επιτυχίας, καθώς προέρχονταν από χάκερς ανατολικών χωρών και ήταν συντεταγμένες σε μέτρια αγγλικά, είχαν εμφανή συντακτικά ή γραμματικά λάθη με εντελώς ερασιτεχνική σχεδίαση που δύσκολα μπορούσε να παραπλανήσει. Σταδιακά, το περιεχόμενο βελτιώθηκε, το κείμενο έγινε πειστικό και η τεχνική σχεδίαση επαγγελματική με αποτέλεσμα ο αριθμός των θυμάτων να αυξηθεί πολύ. Βλ. σχετικά *M. Gercke,* Die Strafbarkeit von " Phishing" und Identitätsdiebstahl, CR 2005, 606.

[37] Σύμφωνα με τα στατιστικά στοιχεία που δημοσιεύονται στην ιστοσελίδα www.antiphishing.org (Φεβρ. 2007), οι χώρες από τις οποίες ενεργούν οι δράστες είναι, κυρίως, η Κίνα και οι ΗΠΑ και ακολουθούν η Ν. Κορέα και διάφορες μεγάλες ευρωπαϊκές χώρες. Κύριος στόχος τέτοιων επιθέσεων είναι ο χώρος των οικονομικών υπηρεσιών (92,6%).

οικονομικός διαχειριστής εισπράττει προμήθεια άκαπα, χωρίς καμιά δική του ενέργεια, ο δε δράστης της απάτης με υπολογιστή διασφαλίζει μέσω της παρεμβολής του τρίτου προσώπου την ανωνυμία του. Σε πολλές από αυτές τις περιπτώσεις ο οικονομικός διαχειριστής δεν είναι πρόσωπο που συμμετέχει εξ αρχής στο εγκληματικό σχέδιο, αλλά τρίτος που απλώς εξασφαλίζει την προμήθειά του πειθόμενος (με σχετική ευκολία) στις διαβεβαιώσεις του δράστη ότι πρόκειται για σοβαρή επένδυση που πρέπει να ξεπεράσει συναλλαγματικά, γραφειοκρατικά και άλλα οργανωτικά προβλήματα.

### 1.4.2. Η οικονομική κατασκοπεία (economic espionage[38])

Η λεγόμενη «οικονομική κατασκοπεία» διευθύνεται και ουσιαστικά ενορχηστρώνεται από τις κυβερνήσεις των κρατών σε διεθνές επίπεδο, ενώ παράλληλα η βιομηχανική ή εταιρική κατασκοπεία είναι συχνότερα εθνική και εμφανίζεται μεταξύ των επιχειρήσεων ή των εταιριών στο εσωτερικό μιας χώρας. Η τεχνολογική εξέλιξη δίνει πλέον απλόχερα τη δυνατότητα σε όσους το επιθυμούν να προβούν στην παράνομη απόκτηση πνευματικής ιδιοκτησίας, ιδεών, τεχνικών και διαδικασιών, συνταγών και τύπων σχετικούς με τη βιομηχανική παραγωγή και κατασκευή ή ακόμη να μπορέσουν να αποκτήσουν πρόσβαση σε αμέτρητο αριθμό ιδιόκτητων ή λειτουργικών πληροφοριών, όπως αυτές για τα σύνολα δεδομένων πελατών, την τιμολόγηση, τις πωλήσεις, το μάρκετινγκ, την έρευνα και την ανάπτυξη, τις πολιτικές, τις ενδεχόμενες προσφορές, τον προγραμματισμό ή τις εμπορικές στρατηγικές ή τις μεταβαλλόμενες συνθέσεις και τις θέσεις της παραγωγής εταιριών και επιχειρήσεων.

Η οικονομική και βιομηχανική κατασκοπεία συνηθέστερα συνδέεται με τις τεχνολογικά-βαριές βιομηχανίες, συμπεριλαμβανομένου αυτές των λογισμικού και υλικών υπολογιστών[39], της βιοτεχνολογίας, του αεροδιαστήματος, των τηλεπικοινωνιών, της τεχνολογίας μεταφορών και μηχανών, των αυτοκινήτων, των μηχανικών εργαλείων, της ενέργειας, των υλικών και των επιστρωμάτων και ούτω καθεξής. Η Silicon Valley[40], είναι

---

[38] http://www.economicespionage.com/, http://en.wikipedia.org/wiki/Industrial_espionage

[39] Για μια τέτοια περίπτωση ηλεκτρονικού εγκλήματος (παραβίαση επιχειρηματικού απορρήτου με αντιγραφή αρχείων από το σκληρό δίσκο ηλεκτρονικού υπολογιστή σε δισκέτα) βλ. ΑΠ 121/2003 Π.Λογ 2003, 161 επ. ΠοινΧρον ΝΓ 910 επ., με παρατ. *Α. Κωνσταντινίδη*

[40] Η **Κοιλάδα του πυριτίου** (Silicon Valley) βρίσκεται στο νότιο τμήμα του Κόλπου του Σαν Φρανσίσκο (San Francisco Bay Area) στη Βόρεια Καλιφόρνια των ΗΠΑ. Ο όρος αρχικά αναφερόταν στον μεγάλο αριθμό των καινοτόμων εταιρειών σχεδίασης μικροκυκλωμάτων (με βάση το πυρίτιο) και τους κατασκευαστές που υπήρχαν

γνωστή ως μια από τις περισσότερο στοχοθετημένες περιοχές για αυτής της μορφής την κατασκοπεία, αλλά, στην πραγματικότητα, οποιαδήποτε βιομηχανία με πληροφορίες προς χρήση από ανταγωνιστές μπορεί να είναι ένας στόχος.

Η άνοδος του Διαδικτύου και των δικτύων υπολογιστών έχει επεκτείνει το εύρος και τη λεπτομέρεια της διαθέσιμης πληροφορίας και την ευκολία της πρόσβασης σε αυτή με απώτερο σκοπό την οικονομική κατασκοπεία. Παγκοσμίως, γύρω στις 50.000 επιχειρήσεις ημερησίως θεωρείται ότι πέφτουν θύματα cyber-attack με το ποσοστό να υπολογίζεται ότι διπλασιάζεται κάθε έτος. Επίσης η αυξανόμενη χρήση του Διαδικτύου έχει μεγιστοποιήσει τις ευκαιρίες της οικονομικής κατασκοπείας με στόχο και το σαμποτάζ. Στις αρχές του 2000, παρατηρήθηκε ότι οι επιχειρήσεις που ασχολούνταν με την ενέργεια γίνονταν όλο και συχνότερα θύματα επιθέσεων από χάκερ. Η χρήση αυτών των μεθόδων κατασκοπείας προκαλεί τα τελευταία χρόνια μια όλο και περισσότερο αυξανόμενη ανησυχία για τις κυβερνήσεις, λόγω των πιθανών επιθέσεων από τρομοκρατικές ομάδες ή εχθρικές ξένες κυβερνήσεις.

Σε νομικό επίπεδο ξεχωρίζει η Economic espionage Act 1996[41] όπου πέρασε από το Κογκρέσο και υπογράφηκε από τον πρόεδρο των ΗΠΑ, Κλίντον, την 11 Οκτωβρίου 1996 και αφορά την προστασία σημαντικών πληροφοριών ορίζοντας παράλληλα πολύ υψηλά πρόστιμα, σε όποιο κράτος, οργανισμό, φορέα ή επιχείρηση διαπράξει παράβαση προβλεπόμενη βάσει των διατάξεων της.

## 2. Συστήματα πληρωμών και μέσα πληρωμών

### 2.1. Εισαγωγικές ορολογικές διευκρινήσεις

Οι σύγχρονες οικονομίες που βασίζονται στον καταμερισμό της εργασίας χαρακτηρίζονται από την ύπαρξη αποτελεσματικών αγορών υπηρεσιών πληρωμών. Τα

στην περιοχή, αλλά τελικά κατέληξε να αναφέρεται σε όλες τις υψηλής τεχνολογίας επιχειρήσεις που εδρεύουν εκεί. Σήμερα γενικά χρησιμοποιείται ως μετωνύμιο για τον τομέα υψηλής τεχνολογίας, που δραστηριοποιούνται στις τεχνολογίες της Πληροφορικής και των Επικοινωνιών - οδηγοί των εξελίξεων σε αυτούς τους τομείς - με ειδικευμένο εργατικό δυναμικό από όλο τον κόσμο

[41] http://www.economicespionage.com/EEA.html

συστήματα[42] και τα μέσα πληρωμών περιβάλλουν την πραγματική οικονομία με ένα "αόρατο χρηματικό πέπλο". Οι πληρωμές επιτρέπουν την ικανοποίηση απαιτήσεων και την τήρηση υποχρεώσεων, την πραγματοποίηση αγορών αγαθών και υπηρεσιών και την υλοποίηση αμέτρητων μεμονωμένων αποφάσεων για αποταμίευση και επένδυση, ή ακόμα και την απλή αποστολή χρημάτων.

Οι υπηρεσίες πληρωμών παρέχονται από πολλούς φορείς. Λόγω της απρόσκοπτης εκτέλεσης ιδιαίτερα μεγάλου αριθμού καθημερινών συναλλαγών, το ευρύ κοινό τείνει να υποεκτιμά την οικονομική λειτουργία των πληρωμών και την προστιθέμενη αξία που αυτές δημιουργούν αδιάλειπτα. Η ύπαρξη υγιών συστημάτων πληρωμών και παρόχων υπηρεσιών πληρωμών ενισχύει την εμπιστοσύνη στο εθνικό νόμισμα και στη σταθερότητα του χρηματοπιστωτικού συστήματος. Σε όλες τις εθνικές οικονομίες, ο αριθμός των απασχολούμενων στον τομέα των υπηρεσιών πληρωμών είναι σημαντικός.

Ο Ευρωπαίος νομοθέτης στην προσπάθειά του να εξασφαλίσει την ευρύτερη δυνατή προστασία στα «μέσα πληρωμής πλην των μετρητών» προβλέπει στο άρθρο 2 την υποχρέωση των κρατών μελών για εγκληματοποίηση ενός ευρέος φάσματος συμπεριφορών με κοινό υλικό αντικείμενο τα μέσα πληρωμής πλην των μετρητών. Ο συγκερασμός σε ενιαίο κείμενο prima facie ανομοιογενών εγκληματικών συμπεριφορών αναδεικνύει την κεντρική σημασία του μέσου πληρωμής. Η διαφορετικότητα των μέσων πληρωμής αφενός και αφετέρου η πολυμορφία των πράξεων πληρωμής, με ή χωρίς την υποστήριξη της τεχνολογίας της πληροφορικής, επιβάλλουν την ορολογική διερκρίνηση των διαφόρων τόπων εγχρήματων συναλλαγών. Η συνοπτική ανάλυση της λειτουργίας και των συμβατικών δομών των εγχρήματων συναλλαγών θα επιτρέψει τον έλεγχο της απόφασης για παροχή αποσπασματικής ποινικής προστασίας σε κάποια από τα «μέσα πληρωμής πλην των μετρητών» σε ευρωπαϊκό και τη διαπίστωση της νομιμότητας και αναγκαιότητας της εφαρμογής της σε εθνικό επίπεδο, με άξονα πάντα το διακυβευόμενο ποινικό έννομο αγαθό.

---

[42] Σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μια περιοχή, συνήθως σε μια χώρα. Υπό την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει: α) τα πιστωτικά ιδρύματα και τους χρηματοδοτικούς οργανισμούς, β) μη πιστωτικά ιδρύματα που παρέχουν υπηρεσίες για τη διενέργεια πληρωμών, γ) την τεχνική υποδομή, δ) το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, ε) τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και στ) τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος. Βλ. Πράξη Συμβουλίου Νομισματικής Πολιτικής, Αριθ. 50/31.7.2002, καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών

## 2.2. Τα συστήματα πληρωμών και τα μέσα πληρωμών.

### 2.2.1. Εισαγωγή στα συστήματα πληρωμών

Τα συστήματα πληρωμών στις μέρες μας, περισσότερο ίσως από κάθε άλλη φορά, αντιμετωπίζουν μεγάλες και σύνθετες προκλήσεις. Το κανονιστικό πλαίσιο που τα διέπει αλλάζει, οι τεχνολογικές υποδομές που τα υποστηρίζουν εξελίσσονται, ο σκοπός τους επεκτείνεται και οι απαιτήσεις της πελατείας των τραπεζών πρέπει να ικανοποιούνται. Αρχικά θα επιχειρηθεί ένας ορολογικός προσδιορισμός της έννοιας των συστημάτων πληρωμών ενώ στη συνέχεια θα γίνει παρουσίαση των προγραμμάτων TARGET που θεσπίστηκαν σε ευρωπαϊκό επίπεδο. Τέλος, θα γίνει αναφορά στην οδηγία 2007/64/ΕΚ[43], για τις υπηρεσίες πληρωμών στην εσωτερική αγορά.

### 2.2.2. Ορολογικός προσδιορισμός

Ως σύστημα πληρωμών ορίζεται το σύνολο των εργαλείων, υπηρεσιών, διαδικασιών και, κατά κανόνα, διατραπεζικών συστημάτων, μέσω των οποίων επιτυγχάνεται η μεταφορά κεφαλαίων μεταξύ των φορέων που συμμετέχουν σε αυτό.[44] Για την εξειδίκευση του εν λόγω ορισμού, απαραίτητες είναι οι ακόλουθες διευκρινίσεις:

**(α)** Ως μεταφορά κεφαλαίων νοείται η μεταφορά κεφαλαίων που λαμβάνει χώρα με τη χρήση όλων των διαθέσιμων εργαλείων πληρωμών και υπηρεσιών μεταφοράς κεφαλαίων βάσει εντολής πληρωμής σύμφωνα με τα προαναφερθέντα στην ενότητα Α της παρούσας μελέτης (υπό 3).

**(β)** Συμμετέχοντες στα συστήματα πληρωμών είναι κυρίως οι τράπεζες (χωρίς να αποκλείονται και οι άλλες κατηγορίες φορέων παροχής χρηματοπιστωτικών υπηρεσιών που έχουν άδεια λειτουργίας για την παροχή υπηρεσιών πληρωμών). Για το λόγο αυτό τα συστήματα πληρωμών είθισται να καλούνται «διατραπεζικά».

**(γ)** Σε ό,τι αφορά τη διαχείριση των συστημάτων πληρωμών δεν υπάρχει κυρίαρχο πρότυπο. Ένα σύστημα πληρωμών μπορεί να τελεί υπό τη διαχείριση:

---

[43] Οδηγία 2007/64/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Νοεμβρίου 2007 «*για τις υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ και 2006/48/ΕΚ, και την κατάργηση της οδηγίας 97/5/ΕΚ*», Ε.Ε. L 319, 5.12.2007, σελ. 1-36

[44] *Βλέπε* σχετικά **Committee on Payment and Settlement Systems (2003a)**, op. cit., σελ. 38.

είτε των κεντρικών τραπεζών,[45]

είτε των κεντρικών τραπεζών σε συνεργασία με τις τράπεζες και τις υπόλοιπες κατηγορίες φορέων παροχής υπηρεσιών πληρωμών,

είτε τέλος μόνον των φορέων παροχής υπηρεσιών πληρωμών.

Σύμφωνα με άλλο ορισμό, σύστημα πληρωμών [46] ορίζεται το σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μια περιοχή, συνήθως σε μια χώρα. Υπό την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει: α) τα πιστωτικά ιδρύματα και τους χρηματοδοτικούς οργανισμούς, β) μη πιστωτικά ιδρύματα που παρέχουν υπηρεσίες για τη διενέργεια πληρωμών, γ) την τεχνική υποδομή, δ) το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, ε) τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και στ) τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος.

Στον όρο «συστήματα πληρωμών» μπορούν παράλληλα να δοθούν και δυο ευρύτερες έννοιες[47]:

Σε κάποιες περιπτώσεις αναφέρεται στο σύνολο των οργάνων, των τραπεζικών διαδικασιών και των διατραπεζικών συστημάτων μεταφοράς κεφαλαίων όπου διευκολύνουν την κυκλοφορία του χρήματος σε γεωγραφική ή νομισματική περιοχή

Στις περισσότερες των περιπτώσεων όμως χρησιμοποιείται για να περιγράψει «το σύστημα μεταφοράς κεφαλαίων», έναν επίσημο πολυμερή διακανονισμό βασισμένο σε ιδιωτική σύμβαση ή νομοθεσία, σε κοινούς κανόνες και τυποποιημένες συμφωνίες, σχετικά με τη μετάδοση, την εκκαθάριση και τη διευθέτηση των οικονομικών υποχρεώσεων που προκύπτουν μεταξύ των μελών του συστήματος αυτού.

---

[45] Πρόκειται για την πρώτη από τις λειτουργίες που επιτελούν οι κεντρικές τράπεζες στα συστήματα πληρωμών και διακανονισμού.

[46] Βλ. Πράξη Συμβουλίου Νομισματικής Πολιτικής, Αριθ. 50/31.7.2002, καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών

[47] ECB, Glossary of terms related to payment, clearing and settlement systems, December 2009

Όλοι οι παραπάνω ορισμοί χαρακτηρίζονται από έντονη συσχέτιση, με τον καθένα να δίνει και κάποιο ιδιαίτερο χαρακτηριστικό στον όρο «σύστημα πληρωμών». Παρακάτω θα επιχειρηθεί μια κατηγοριοποίηση των συστημάτων πληρωμών όπως και αυτών της εκκαθάρισης και διακανονισμού των πληρωμών.

### 2.2.3. Κατηγοριοποίηση των συστημάτων πληρωμών και των συστημάτων εκκαθάρισης και διακανονισμού πληρωμών

#### 2.2.3.1. Συστήματα πληρωμών

Σύμφωνα με τα ακόλουθα έξι (6) κριτήρια, τα συστήματα πληρωμών διακρίνονται στις εξής κατηγορίες:[48]

(α) Ανάλογα με το εργαλείο πληρωμών ή την υπηρεσία που χρησιμοποιείται για τη μεταφορά κεφαλαίων γίνεται διάκριση ανάμεσα σε συστήματα επιταγών, συστήματα μεταφοράς πιστώσεων,[49] συστήματα άμεσων χρεώσεων,[50] συστήματα καρτών, και συστήματα ηλεκτρονικού χρήματος.

---

[48] Βλέπε σχετικά Committee on Payment and Settlement Systems (2006): General guidance for national payment system development, Bank for International Settlements, January, διαθέσιμο στην ακόλουθη ηλεκτρονική διεύθυνση: http://www.bis.org/publ/cpss70.htm.

[49] Στο πεδίο αυτό συναντώνται τρεις διαφορετικές περιπτώσεις ανάλογα με τον αριθμό των πληρωτών και των δικαιούχων:

(α) Στην πρώτη περίπτωση, ο πληρωτής εντέλλεται την τράπεζά του για τη μεταφορά κεφαλαίων στον τραπεζικό λογαριασμό ενός και μόνον δικαιούχου.

(β) Στη δεύτερη περίπτωση, ο πληρωτής εντέλλεται την τράπεζά του για τη μεταφορά κεφαλαίων στον τραπεζικό λογαριασμό περισσοτέρων δικαιούχων (π.χ. καταβολή συντάξεων από έναν οργανισμό στους δικαιούχους συνταξιούχους).

(γ) Στην τρίτη περίπτωση περισσότεροι πληρωτές εντέλλονται τις τράπεζές τους για τη μεταφορά κεφαλαίων στον τραπεζικό λογαριασμό ενός δικαιούχου (π.χ. καταβολή εργοδοτικών εισφορών από τους υπόχρεους σε ασφαλιστικό οργανισμό).

[50] Στο πεδίο αυτό συναντώνται δύο διαφορετικές περιπτώσεις, ανάλογα τη ροή της εξουσιοδότησης από τον πληρωτή στο δικαιούχο:

(α) Στην πρώτη περίπτωση, ο πληρωτής εξουσιοδοτεί τον δικαιούχο ή την τράπεζα του δικαιούχου, είτε εφάπαξ είτε βάσει πάγιας εντολής, να αναλαμβάνει ποσά από τον τραπεζικό λογαριασμό του και να πιστώνονται σε τραπεζικό λογαριασμό του δικαιούχου για την εκπλήρωση χρηματικής υποχρέωσης του πληρωτή προς τον δικαιούχο (π.χ. εφάπαξ ή πάγια εντολή άμεσης χρέωσης για την εξόφληση λογαριασμών οργανισμών κοινής ωφέλειας).

(β) Στη δεύτερη περίπτωση, η εξουσιοδότηση δίνεται από τον πληρωτή στην τράπεζά του.

(β) Ανάλογα με τον τρόπο με τον οποίο το σύστημα επεξεργάζεται τις εντολές πληρωμών γίνεται διάκριση ανάμεσα σε συστήματα ηλεκτρονικής διαχείρισης και συστήματα χειρόγραφης διαχείρισης.[51]

(γ) Ανάλογα με την αξία των κεφαλαίων που μεταφέρονται, ανά συναλλαγή, μέσα από το σύστημα γίνεται διάκριση ανάμεσα σε:

συστήματα πληρωμών μεγάλης αξίας ("large value payment systems"), και

συστήματα πληρωμών μικρής αξίας ("small value payment systems") ή συστήματα πληρωμών λιανικής ("retail payment systems").[52]

(δ) Ανάλογα με τον αριθμό των συμμετεχόντων στο σύστημα γίνεται διάκριση ανάμεσα σε διμερή συστήματα πληρωμών, και πολυμερή συστήματα πληρωμών.

(ε) Διάκριση γίνεται, επίσης, ανάμεσα σε:

«συστημικώς σημαντικά συστήματα πληρωμών»,[53] δηλαδή συστήματα στα οποία η επέλευση μιας δυσλειτουργίας μπορεί να ενεργοποιήσει ή να μεταδώσει είτε περαιτέρω δυσλειτουργίες μεταξύ των συμμετεχόντων είτε συστημικές δυσλειτουργίες στο σύνολο του χρηματοπιστωτικού συστήματος,[54] και «συστημικώς μη σημαντικά συστήματα πληρωμών», δηλαδή συστήματα τα οποία δεν πληρούν την προαναφερθείσα ιδιότητα.

(στ) Διάκριση γίνεται, τέλος, ανάμεσα στα «αμιγή» συστήματα πληρωμών, μέσω των οποίων λαμβάνει χώρα αποκλειστικά και μόνον η μεταφορά κεφαλαίων μεταξύ των συμμετεχόντων, και τα συστήματα πληρωμών που λειτουργούν στο πλαίσιο ενός συστήματος εκκαθάρισης και διακανονισμού κινητών αξιών για την εκκαθάριση και τον διακανονισμό του σκέλους που αφορά την πληρωμή για την αγορά των κινητών αξιών.[55]

---

[51] Χειρόγραφη διαχείριση γίνεται πλέον μόνον σε ορισμένα συστήματα επιταγών, τα οποία, όπως έχει μόλις προαναφερθεί, είναι τα μοναδικά που επεξεργάζονται εργαλεία πληρωμών που αποτελούν αξιόγραφα ("paper-based instruments").

[52] Το κριτήριο οριοθέτησης μεταξύ των εν λόγω συστημάτων είναι συμβατικό. Κατά κανόνα πάντως, ως συστήματα πληρωμών μεγάλης αξίας νοούνται τα συστήματα μεταφοράς πιστώσεων μέσω των οποίων λαμβάνει χώρα η μεταφορά αξίας που υπερβαίνει, ανά συναλλαγή, το ισόποσο των 50.000 ευρώ.

[53] Αντιπροσωπευτικό παράδειγμα τέτοιων συστημάτων αποτελούν τα συστήματα πληρωμών μεγάλης αξίας.

[54] Βλέπε σχετικά **Committee on Payment and Settlement Systems (2001)**: Core Principles for Systemically Important Payment Systems, Bank for International Settlements, January (διαθέσιμο στην ακόλουθη ηλεκτρονική διεύθυνση: http://www.bis.org/publ/cpss43.htm), σελ. 5.

[55] Βλέπε σχετικά αμέσως κατωτέρω, υπό 3.

### 2.2.3.2. Συστήματα εκκαθάρισης και διακανονισμού πληρωμών

Τα συστήματα εκκαθάρισης και διακανονισμού πληρωμών διακρίνονται σε τρεις (3) κατηγορίες, ανάλογα με τον τρόπο που έχει επιλεγεί για τον διακανονισμό των εντολών που αφορούν τη μεταφορά των κεφαλαίων. Ειδικότερα:

(α) Ως συστήματα διακανονισμού σε καθαρή βάση ("net settlement systems") νοούνται εκείνα στα οποία ο διακανονισμός γίνεται με συμψηφισμό και εκκαθάριση του συνόλου των εκατέρωθεν απαιτήσεων των συμμετεχόντων στο σύστημα σε ένα ή περισσότερα χρονικά σημεία της εργάσιμης ημέρας (γνωστά ως «κύκλοι διακανονισμού») κατά τα οποία λαμβάνει χώρα ο διακανονισμός.[56]

(β) Ως συστήματα διακανονισμού σε ατομική ή ακαθάριστη βάση ("gross settlement systems") νοούνται εκείνα στα οποία ο διακανονισμός γίνεται για κάθε πληρωμή χωριστά, χωρίς συμψηφισμό, σε ένα ή περισσότερα χρονικά σημεία της εργάσιμης ημέρας.[57]

(γ) Ως συστήματα διακανονισμού σε ακαθάριστη βάση και πραγματικό χρόνο ("real-time gross settlement systems") νοούνται εκείνα στα οποία ο διακανονισμός γίνεται όχι μόνον για κάθε πληρωμή χωριστά, αλλά και σε πραγματικό χρόνο με τη χρονική σειρά με την οποία δίδονται οι σχετικές εντολές.[58]

*Αμέσως παρακάτω θα εξετασθεί ένα αντιπροσωπευτικό παράδειγμα τέτοιου συστήματος όπως είναι το σύστημα TARGET (Transnational Automated Real-time Gross Settlement Express Transfer System), μέσω του οποίου πραγματοποιείται, μεταξύ άλλων, ο διακανονισμός των πληρωμών που προκύπτουν από πράξεις ανοικτής αγοράς στο πλαίσιο της εφαρμογής της ενιαίας νομισματικής πολιτικής του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών.*[59]

### 2.2.3.3. Τα ευρωπαϊκά προγράμματα TARGET

Η Τράπεζα της Ελλάδος έχει σαφείς αρμοδιότητες στον τομέα των συστημάτων πληρωμών σύμφωνα με το καταστατικό[60] της, το οποίο έχει εναρμονιστεί με το καταστατικό

---

[56] *Βλέπε* σχετικά **Committee on Payment and Settlement Systems (2003a)**, op. cit., σελ. 34.

[57] *Ibid*, σελ. 25.

[58] Ibid, σελ. 41 (βλέπε, επίσης, αναλυτικά **Committee on Payment and Settlement Systems** (1997): Real-time Gross Settlement Systems, March, διαθέσιμο στην ακόλουθη ηλεκτρονική διεύθυνση: http://www.bis.org/publ/cpss22.htm.

[59] Για το εν λόγω σύστημα, βλέπε **Geva, B. (2008)**, σελ. 113-123.

[60] Τράπεζα της Ελλάδος, Καταστατικό, Έκδοση Θ΄, Αθήνα 2000, Βλ. ηλεκτρ. http://www.bankofgreece.gr/BoGDocuments/Καταστατικό_Έκδοση_Θ.pdf

του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών και της Ευρωπαϊκής Κεντρικής Τράπεζας. Στο πλαίσιο αυτό, δύναται να θέτει κανόνες λειτουργίας και να επιβλέπει συστήματα πληρωμών και συστήματα εκκαθάρισης εξωχρηματιστηριακών συναλλαγών, με στόχο την αποτελεσματικότητα και αξιοπιστία τους και ιδίως τον περιορισμό του συστημικού κινδύνου και την ενίσχυση του ανταγωνισμού. Επίσης, να διαχειρίζεται τέτοια συστήματα, επιφυλασσομένων των διατάξεων που ισχύουν κάθε φορά στο πλαίσιο του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών.

- TARGET

Σε επίπεδο Ευρωπαϊκής Ένωσης ήδη από το 1999 άρχισε να λειτουργεί το σύστημα TARGET, το οποίο απαρτιζόταν από τα εθνικά συστήματα διακανονισμού πληρωμών σε συνεχή χρόνο των κρατών-μελών της ΕΕ που συμμετείχαν στην ΟΝΕ, το μηχανισμό πληρωμών της Ευρωπαϊκής Κεντρικής Τράπεζας και το μηχανισμό διασύνδεσής τους. Στο TARGET, όπως και στο TARGET 2, είχαν τη δυνατότητα να συνδεθούν και τα συστήματα πληρωμών των χωρών της ΕΕ που δεν είχαν υιοθετήσει το ευρώ. Στο πλαίσιο αυτό, η Ελλάδα συμμετείχε στο TARGET από την έναρξη λειτουργίας του με το σύστημα πληρωμών ΕΡΜΗΣ.

Το TARGET[61], αρχικά του "Trans-European Automated Real-time Gross Express Transfer system" ονομάζεται το σύστημα διακανονισμού εντολών πληρωμής μεγάλων ποσών σε συνεχή χρόνο για το Ευρώ, δηλαδή υπό κανονικές συνθήκες οι πληρωμές φθάνουν στον προορισμό τους σε ελάχιστα λεπτά, αν όχι δευτερόλεπτα, αφ' ότου χρεωθεί ο λογαριασμός του αποστέλλοντος μέλους και φυσικά όλες οι πληρωμές έχουν την ίδια μεταχείριση ανεξάρτητα από την αξία τους. Δημιουργήθηκε για να επιτύχει τρεις κύριους στόχους: α) Να παράσχει έναν ασφαλή και αξιόπιστο μηχανισμό για το διακανονισμό διασυνοριακών πληρωμών, με βάση το διακανονισμό σε συνεχή χρόνο, β) να αυξήσει την αποτελεσματικότητα των διασυνοριακών πληρωμών μεταξύ των χωρών- μελών της ΕΕ, και προπάντων, γ) να εξυπηρετήσει τις ανάγκες της νομισματικής πολιτικής του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών (ΕΣΚΤ).

[61] http://www.ecb.de/pub/pdf/other/tagiel_bel.pdf

- TARGET 2

Το TARGET 2[62] είναι το νέο διευρωπαϊκό σύστημα πληρωμών, το οποίο αντικατέστησε το σύστημα TARGET. Η ανάπτυξη του νέου συστήματος οφείλεται στις απαιτήσεις που δημιουργήθηκαν τόσο από τη διεύρυνση της Ευρωπαϊκής Ένωσης (ΕΕ) και τις τεχνολογικές εξελίξεις όσο και από τις αγορές, για ασφαλή και αποτελεσματική λειτουργία των συστημάτων και εναρμονισμένες υπηρεσίες πληρωμών σε όλη την Ευρώπη. Στο TARGET 2, μια ενιαία τεχνική πλατφόρμα (Ενιαία Κοινή Πλατφόρμα-ΕΚΠ) παρέχεται από τις κεντρικές τράπεζες της Γερμανίας, της Γαλλίας και της Ιταλίας, αντικαθιστώντας την αποκεντρωμένη δομή του αρχικού συστήματος TARGET. Με το TARGET 2, το Ευρωσύστημα προσφέρει υπηρεσίες με ενιαία τιμολόγηση των πληρωμών τόσο εντός όσο και μεταξύ των κρατών-μελών που συμμετέχουν σε αυτό, με γνώμονα την ανάκτηση του κόστους.

Το TARGET2 προσφέρει μεγάλο εύρος υπηρεσιών για να καλύψει τις απαιτήσεις όλων των χρηστών (ευρωπαϊκού τραπεζικού τομέα, Εθνικών Κεντρικών Τραπεζών και Ευρωπαϊκής Κεντρικής Τράπεζας). Η ενιαία πλατφόρμα του TARGET 2 υποστηρίζει την ομογενοποίηση των εργασιών των τραπεζών, η οποία συμβάλλει στην ομαλή και αποτελεσματική επεξεργασία των πληρωμών. Επιπλέον, το TARGET 2 διαθέτει προηγμένα μέσα διαχείρισης της ρευστότητας καθώς και εναρμονισμένες διαδικασίες για τον διακανονισμό των επικουρικών συστημάτων, δηλαδή των συμψηφιστικών συστημάτων και των συστημάτων διακανονισμού χρεογράφων. Το TARGET 2 προσφέρει, επίσης, το υψηλότερο δυνατό επίπεδο αξιοπιστίας, καθώς και προηγμένους μηχανισμούς για τη συνέχιση των εργασιών.

Η μετάπτωση στο TARGET 2 πραγματοποιήθηκε σταδιακά για τρεις ομάδες χωρών, με την πρώτη να συνδέεται στις 19 Νοεμβρίου 2007, ημερομηνία έναρξης λειτουργίας του συστήματος. Η δεύτερη ομάδα συνδέθηκε στις 18 Φεβρουαρίου 2008 και η τρίτη στις 19 Μαΐου 2008[63]

Η λειτουργία του TARGET 2 κρίνεται ως ιδιαίτερα επιτυχής. Για την περίοδο Ιανουαρίου – Σεπτεμβρίου 2009, ο όγκος και η αξία των πληρωμών που διακανονίστηκαν στο

[62] http://www.bankofgreece.gr/Pages/el/PaymentsSystems/largepayments.aspx

[63] Η εν λόγω ημερομηνία είναι αυτή από την οποία και έπειτα συμμετέχει και η Ελλάδα.

σύστημα TARGET 2- GR ήταν, σε ημερήσια βάση 330.000 εντολές αξίας €1,91 τρισεκ. Η διαθεσιμότητα του συστήματος κινήθηκε σε πολύ υψηλά επίπεδα, ενώ το σύστημα ανταποκρίθηκε ικανοποιητικά και τις ημέρες κατά τις οποίες παρουσιάστηκε αυξημένος όγκος συναλλαγών.

Η συνεργασία του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών με τις τράπεζες, μέσω εκτεταμένων διαβουλεύσεων, η οποία διευκόλυνε την ομαλή μετάπτωση στο νέο σύστημα, συμβάλλει στη συνεχή βελτίωση του συστήματος και στην εισαγωγή νέων λειτουργιών. Η πρώτη έκδοση του συστήματος TARGET 2 που υποστηρίζει τις νέες δυνατότητες λειτουργεί από τον Νοέμβριο 2008. Δύο επιπλέον εκδόσεις του τέθηκαν σε λειτουργία το 2009, ενώ για το Νοέμβριο του 2010 προγραμματίζεται η εισαγωγή νέας έκδοσης του TARGET 2.

### 2.2.4. Η Οδηγία 2007/64 για τις υπηρεσίες πληρωμών στην εσωτερική αγορά

Σε κοινοτικό επίπεδο, από της 13ης Νοεμβρίου 2007 έχει εκδοθεί η Οδηγία 2007/64 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ και 2006/48/ΕΚ, και την κατάργηση της οδηγίας 97/5/ΕΚ. Η παρούσα οδηγία εφαρμόζεται στις υπηρεσίες πληρωμών που παρέχονται εντός της Κοινότητας. Εντούτοις, με την εξαίρεση του άρθρου 73, οι τίτλοι ΙΙΙ και IV εφαρμόζονται μόνο όταν τόσο ο πάροχος υπηρεσιών πληρωμών του πληρωτή όσο και ο πάροχος υπηρεσιών πληρωμών του δικαιούχου, ή ο μοναδικός πάροχος υπηρεσιών πληρωμών για την πράξη πληρωμής, είναι εγκατεστημένοι στην Κοινότητα

Η έκδοση της Οδηγίας 2007/64/ΕΚ, αποτελεί μια ιδιαίτερα σημαντική πρωτοβουλία στον τομέα των πληρωμών για τρεις κυρίως λόγους[64]:

- Πρώτον, λαμβανομένων υπόψη του αποσπασματικού μέχρι την έκδοσή της πλαισίου που διέπει σε κοινοτικό επίπεδο τις πληρωμές και των εξελίξεων που επήλθαν με την εισαγωγή του Ενιαίου Χώρου Πληρωμών σε ευρώ (SEPA)[65], είναι ιδιαίτερα σημαντικό ότι με την

[64] Χρήστος Βλ. Γκόρτσος, Άρθρο, Η Οδηγία 2007/64/ΕΚ για τις υπηρεσίες πληρωμών στην εσωτερική αγορά - Συνολική θεώρηση, Οικονομική επιθεώρηση 2009

[65] Ο SEPA είναι ένας χώρος στον οποίο οι καταναλωτές, οι εταιρίες και οι λοιποί οικονομικοί παράγοντες θα είναι σε θέση να διενεργούν και να δέχονται εγχώριες και διασυνοριακές πληρωμές σε ευρώ με τους ίδιους βασικούς όρους και τα ίδια δικαιώματα και υποχρεώσεις ανεξάρτητα από τη γεωγραφική τους θέση. Σκοπός του

Οδηγία αυτή επιχειρείται η θέσπιση σε κοινοτικό επίπεδο ενός σύγχρονου και συνεκτικού νομικού πλαισίου για τις υπηρεσίες πληρωμών που λαμβάνει ταυτόχρονα υπόψη τις απαιτήσεις που πρέπει να πληρούνται για τη δυνατότητα παροχής υπηρεσιών πληρωμών στο πλαίσιο του SEPA.

- Δεύτερον, με την Οδηγία αυτή προσδιορίζονται όλες οι κατηγορίες φορέων παροχής υπηρεσιών πληρωμών που μπορούν νόμιμα να παρέχουν υπηρεσίες πληρωμών στην Κοινότητα, όπως ενδεικτικά, τα πιστωτικά ιδρύματα και τα ιδρύματα ηλεκτρονικού χρήματος, ενώ εισάγεται και μια νέα κατηγορία φορέων παροχής υπηρεσιών πληρωμών, τα καλούμενα «ιδρύματα πληρωμών», για τα οποία προβλέπονται συγκεκριμένες προϋποθέσεις αδειοδότησης και άσκησης δραστηριότητας κατά την παροχή εκ μέρους τους υπηρεσιών πληρωμών.

- Τρίτον, καθορίζονται διεξοδικά αφενός μεν οι κανόνες διαφάνειας και οι υποχρεώσεις ενημέρωσης που πρέπει να τηρούνται σχετικά με τις υπηρεσίες πληρωμών και αφετέρου τα δικαιώματα και οι υποχρεώσεις των χρηστών υπηρεσιών πληρωμών και των παρεχόντων αυτές ως τακτική απασχόληση ή επιχειρηματική δραστηριότητα.

Τέλος, κρίνεται σκόπιμο να επισημανθεί ότι οι εν λόγω διατάξεις της Οδηγίας είναι ιδιαίτερα διεξοδικές, καθώς ρυθμίζουν κάθε επιμέρους περίπτωση ξεχωριστά, εισάγοντας πολύ σημαντικά δικαιώματα για τον καταναλωτή-χρήστη υπηρεσιών πληρωμών και ιδιαίτερα αυξημένες υποχρεώσεις αντίστοιχα για τους φορείς παροχής υπηρεσιών πληρωμών.

## 2.3. Έννοια των μέσων πληρωμής

Η απόφαση-πλαίσιο 2001/413 του Συμβουλίου[66] κάνει λόγο ήδη στον τίτλο της για «μέσα πληρωμής πλην των μετρητών» (cashless means of payment - öbargeldlose Zahlungsmittel). Ως τέτοιο μέσο πληρωμής ορίζεται[67] «κάθε ενσώματο μέσο, εκτός από το νόμιμο νόμισμα (τραπεζογραμμάτια και κέρματα) που επιτρέπει, λόγω της ιδιαίτερης φύσης

SEPA είναι η δημιουργία μιας ενοποιημένης, ανταγωνιστικής και καινοτόμου αγοράς πληρωμών μικρής αξίας στον ευρωπαϊκό χώρο, όπου οι πληρωμές σε ευρώ χωρίς μετρητά θα διενεργούνται με τη χρήση ενός μόνο τραπεζικού λογαριασμού και μιας ενιαίας δέσμης μέσων πληρωμών.

[66] *Επίσημη Εφημερίδα αριθ. L 149 της 02/06/2001 σ. 0001 - 0004*

[67] Βλ. άρθρο 1 στοιχ. Α' απόφαση-πλαίσιο 2001/413

του, μόνο του ή σε συνδυασμό με άλλο μέσο (πληρωμής), στον κάτοχο ή στο χρήστη του να μεταφέρει χρήματα ή νομισματική αξία (...) και που προστατεύεται από την απομίμηση ή τη δόλια χρήση, παραδείγματος χάριν μέσω σχεδιασμού, κωδικού ή υπογραφής». Απαραίτητο τεχνικό χαρακτηριστικό των μέσων πληρωμής αποτελεί επομένως η προστασία τους από την απομίμηση ή τη δόλια χρήση. Ως μέσα πληρωμής που εμπίπτουν στο πεδίο εφαρμογής της απόφασης-πλαισίου απαριθμούνται ενδεικτικά στο άρθρο 1 στοιχ. α' οι πιστωτικές κάρτες, οι κάρτες των ευρωεπιταγών, άλλες κάρτες εκδιδόμενες από χρηματοπιστωτικά ιδρύματα, οι ταξιδιωτικές επιταγές, οι ευρωεπιταγές και εν γένει οι επιταγές και οι συναλλαγματικές.

Άμεσος οικονομικός σκοπός των μέσων πληρωμής είναι η διενέργεια «πράξεων πληρωμής», δηλαδή η μεταφορά χρημάτων ή νομισματικής αξίας. Η πράξη πληρωμής μπορεί να έγκειται πέρα από την πραγματοποίηση πληρωμής για αγαθά ή υπηρεσίες (π.χ. με την χρήση πιστωτικής κάρτας) και στην ανάληψη χρημάτων (πχ. σε Αυτόματες Ταμειολογιστικές Μηχανές) ή στην έκδοση εντολής μεταφοράς χρημάτων (υπό μορφή χρηματικής απαίτησης έναντι τρίτου) σε διαταγή δικαιούχου (πχ. με την έκδοση επιταγής).

Στο άρθρο 2 της απόφασης-πλαισίου προβλέπεται η υποχρέωση των κρατών μελών για εγκληματοποίηση μιας σειράς εκ προθέσεως τελουμένων πράξεων, «τουλάχιστον όσον αφορά τις πιστωτικές κάρτες, τις κάρτες ευρωεπιταγών, λοιπές κάρτες εκδιδόμενες από χρηματοπιστωτικά ιδρύματα, τις ταξιδιωτικές επιταγές, τις ευρωεπιταγές, λοιπές επιταγές και συναλλαγματικές». Για τα αδικήματα που αφορούν αυτά τα μέσα πληρωμής, τα οποία ταυτίζονται με τα αναφερόμενα ενδεικτικά στο άρθρο 1, υποχρεούται ο Έλληνας νομοθέτης να προβλέψει σύμφωνα με το άρθρο 6 της απόφασης-πλαίσιου αποτελεσματικές, ανάλογες και αποτρεπτικές ποινές. Τουλάχιστον στις βαριές περιπτώσεις δεν αρκεί η πρόβλεψη χρηματικών ποινών αλλά απαιτούνται στερητικές της ελευθερίας ποινές.

Για τα αδικήματα που αφορούν άλλα μέσα πληρωμής εναπόκειται επομένως στη διακριτική ευχέρεια του εκάστοτε κράτους μέλους η επιλογή μεταξύ αφενός αυστηρής ποινής και αφετέρου αποτελεσματικής, ανάλογης και αποτρεπτικής μεν, επιεικούς δε, διοικητικής κύρωσης. Τέτοια μέσα ηλεκτρονικής πληρωμής που ο εθνικός νομοθέτης δύναται αλλά δεν υποχρεούται να αναγάγει σε υλικό αντικείμενο των σχετικών εγκλημάτων είναι π.χ. οι κάρτες που δεν εκδίδονται από χρηματοπιστωτικά ιδρύματα. Στην κατηγορία αυτή υπάγονται π.χ. οι προπληρωμένες κάρτες απλής (και όχι πολλαπλής) χρήσεως, όπως οι τηλεφωνικές κάρτες (τηλεκάρτες), τις οποίες εκδίδουν επιχειρήσεις τηλεφωνίας και όχι τράπεζες. Ακατάλληλο

υλικό αντικείμενο των εγκλημάτων του άρθρου 2 αποτελούν και άλλα μέσα ηλεκτρονικής πληρωμής υπό την προεκτεθείσα ευρεία έννοια του όρου, που αν και υποστηρίζουν τη διενέργεια πληρωμών εξ αποστάσεως π.χ. μέσω τηλεφώνου (phone banking) ή κατ' οίκον μέσω διαδικτύου (home-internet banking), εντούτοις δεν αποτελούν κατάλληλα μέσα πληρωμής κατά τον ορισμό του άρθρου 1 της απόφασης-πλαισίου, ελλείψει ενσώματου χαρακτήρα. Οι μορφές αυτές πράξεων ηλεκτρονικής πληρωμής αποκτούν ωστόσο ποινικό ενδιαφέρον στα πλαίσια του άρθρου 3 (αδικήματα που σχετίζονται με τους υπολογιστές).

Τα παραπάνω ηλεκτρονικά και αξιογραφικά μέσα πληρωμής αποτελούν καθαυτά το υλικό αντικείμενο των επιμέρους εγκληματικών συμπεριφορών του άρθρου 2 που στόχο έχει την προστασία της λειτουργικότητας των εγχρήματων με ευρεία έννοια συναλλαγών.

## 2.4. Έννοια και μορφές του χρήματος

Τη βάση της σημερινής ανταλλακτικής, πολλώ μάλλον καπιταλιστικής και παγκοσμιοποιημένης οικονομίας, αποτελούν κατά γενική ομολογία οι χρηματικές ενοχές. Από οικονομική σκοπιά το χρήμα είναι ένα μέσο για την εκπλήρωση σκοπών οικονομικής φύσεως. Οι οικονομικές λειτουργίες συνοψίζονται στη χρηστικότητα του ως μέσου για την εκπλήρωση υποχρεώσεων αλλά και ως φορέα αξίας και μέτρου αξιών. Η οικονομική θεώρηση του χρήματος, στην οποία δεσπόζουσα θέση έχει η συναλλακτική του λειτουργία αποτυπώνεται στον νομικό ορισμό του χρήματος υπό ευρεία έννοια: Ως χρήμα υπό ευρεία έννοια νοείται οποιοδήποτε υλικό αντικαταστατό αντικείμενο χρησιμοποιείται ως κοινό ανταλλακτικό μέσο για την απόκτησή αγαθών ή υπηρεσιών. Προϋπόθεση του χρήματος είναι επομένως η σχετικά ευρεία κυκλοφορία του ή κατ' άλλη διατύπωση η ιδιότητα του ως γενικού μέσου πληρωμών.

Την οικονομική αυτή λειτουργία εκπληρώνει παραδοσιακά το νόμισμα της κάθε πολιτείας ως χρήμα υπό τη στενή έννοια του όρου. Νόμισμα υπό τη στενή έννοια του όρου είναι τα χαρτονομίσματα (τραπεζογραμμάτια) ή μεταλλικά κέρματα τα οποία εκδίδονται από το κράτος και τα οποία ως φορείς αξίας και μέσα πληρωμής κυκλοφορούν νόμιμα. Σε διάφορες κοινωνίες και περιόδους το ρόλο ευρέως εννοούμενου χρήματος έχουν παίξει και άλλα πράγματα όπως π.χ. ο χρυσός, ο άργυρος ή το λάδι. Οι σύγχρονες οικονομίες ανταποκρινόμενες στην ανάγκη για ταχύτητα, χαμηλό κόστος και ασφάλεια πληρωμών ήρθαν

να προσθέσουν νέες μορφές ευρέως εννοούμενου χρήματος: αρχικά το λογιστικό, αργότερα το πλαστικό και πρόσφατα το ηλεκτρονικό χρήμα[68].

Η επιταγή και η συναλλαγματική αποτελούν διαδεδομένες μορφές λογιστικού χρήματος. Τα αξιόγραφα αυτά επειδή ενσωματώνουν απαιτήσεις για χρηματική παροχή (χρηματόγραφα) μπορούν να χαρακτηρισθούν και ως «αξιογραφικό νόμισμα». Το λογιστικό χρήμα είναι το συνηθέστερο μέσο υψηλόποσων πληρωμών. Με τον όρο πλαστικό χρήμα περιγράφονται οι τραπεζικές κάρτες με κυριότερες τις πιστωτικές. Ως κάρτα ορίζεται το πλαστικό δελτίο που επιτρέπει στον κάτοχό του να πραγματοποιεί πληρωμή σε κάποιο σημείο πώλησης, ανάληψη ή κατάθεση χαρτονομισμάτων και συναφείς πράξεις σε μηχανές ανάληψης χρημάτων ή αυτόματες ταμειολογιστικές μηχανές. Υπάρχουν και κάρτες των οποίων η μοναδική λειτουργία έγκειται στην εγγύηση των πληρωμών που γίνονται με επιταγές. Η κάρτα χορηγείται από τον εκδότη στον κάτοχο βάσει σύμβασης. Όταν ο εκδότης είναι, ως συνήθως, πιστωτικό ίδρυμα (τράπεζα), πρόκειται για τραπεζική κάρτα. Οι κάρτες δεν είναι αξιόγραφο αλλά μέσο νομιμοποίησης του κομιστή και του κατόχου του λογαριασμού.

## 2.5. Είδη καρτών πληρωμής και ηλεκτρονική τραπεζική

Με βάση τις λειτουργίες τους διακρίνουμε τα εξής είδη τραπεζικών καρτών:

α) την κάρτα αυτόματων αναλήψεων (cash card), που επιτρέπει στους κατόχους να αναλαμβάνουν (και να καταθέτουν) χρήματα από τα μηχανήματα αυτόματης ανάληψης, γνωστά και ως Αυτόματες Ταμειολογιστικές Μηχανές (Automated Teller Machines-ATMs), β) την χρεωστική κάρτα (debit card), που επιτρέπει στον κάτοχό της την αγορά προϊόντων ή υπηρεσιών από συμβεβλημένες με την εκδότρια τράπεζα επιχειρήσεις χωρίς την καταβολή μετρητών αλλά με απλή χρέωση του καταθετικού λογαριασμού που τηρεί ο κάτοχος στην τράπεζα, γ) την πιστωτική κάρτα (credit card), που εκδίδεται συνήθως από τράπεζα και παρέχει στον κάτοχό της τη δυνατότητα να προμηθεύεται πράγματα ή υπηρεσίες από

[68] Νομισματική αξία που συνιστά απαίτηση έναντι του εκδότη, είναι αποθηκευμένη σε ηλεκτρονικό απόθεμα (κάρτα ή λογισμικό), έχει εκδοθεί έναντι καταβολής χρηματικού ποσού, χωρίς απαραίτητα την κίνηση τραπεζικών λογαριασμών και γίνεται δεκτή ως μέσο πληρωμής από επιχειρήσεις άλλες από αυτή της εκδότριας

Βλ. Πράξη Συμβουλίου Νομισματικής Πολιτικής, Αριθ. 50/31.7.2002, καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών

επιχείρηση συμβεβλημένη με τον εκδότη της κάρτας χωρίς άμεση πληρωμή, δηλαδή με πίστωση του ανταλλάγματος. Οι πιστωτικές κάρτες λειτουργούν με βάση μια τριγωνική (τριπρόσωπη) σχέση ανάμεσα στον εκδότη της κάρτας (τράπεζα), τον κάτοχο (καταναλωτή) και τον επιχειρηματία (έμπορο). Η τράπεζα αναλαμβάνει την υποχρέωση να εξοφλεί τις από τον κάτοχο της κάρτας, εντός του συμφωνηθέντος ορίου, αναλαμβανόμενες υποχρεώσεις πληρωμής έναντι των συμβεβλημένων με την τράπεζα επιχειρήσεων, από τις οποίες ο κάτοχος αποκτά αγαθά ή υπηρεσίες. Για την εγγυητική αυτή λειτουργία που αναλαμβάνει η τράπεζα έναντι των συμβεβλημένων επιχειρήσεων (εμπόρων) εισπράττει η τράπεζα αμοιβή από τον κάτοχο (ετήσια συνδρομή) και προμήθεια από τις επιχειρήσεις δ) τις προπληρωμένες κάρτες πολλαπλών χρήσεων, γνωστές και ως «έξυπνες» κάρτες (smart card), οι οποίες αποτελούν το λεγόμενο «ηλεκτρονικό» χρήμα με τη στενή έννοια.

Επειδή οι παραπάνω κάρτες πληρωμής στηρίζουν τη λειτουργία τους στη διαβίβαση και επεξεργασία στοιχείων και δεδομένων με τη χρήση σύγχρονων τηλεπικοινωνιακών μέσων και της τεχνολογίας της πληροφορικής, μπορεί στο εξής να γίνεται αναφορά σε αυτές ως «μέσα ηλεκτρονικής πληρωμής» ή «ηλεκτρονικά μέσα πληρωμής» ή ηλεκτρονικό χρήμα, με ευρεία έννοια. Τα ηλεκτρονικά μέσα πληρωμής μαζί με το αξιογραφικό νόμισμα (επιταγές και συναλλαγματικές) χαρακτηρίζονται και ως «μέσα πληρωμής με πρόσβαση εξ αποστάσεως» επειδή επιτρέπουν στον κάτοχό τους να διαθέτει, από απόσταση και όχι με τους παραδοσιακούς, συμβατικούς τρόπους τραπεζικής εντολής και εκτέλεσης, ποσά που υπάρχουν σε τραπεζικό λογαριασμό του.

Νέες τεχνικές διενέργειας συναλλαγών εξ αποστάσεως επιτρέπει πλέον κατ' εξοχήν και το διαδίκτυο, το οποίο αναδεικνύεται σε λαμπρό πεδίο εφαρμογών «ηλεκτρονικής τραπεζικής» (e-banking). Αρκεί ένας ηλεκτρονικός υπολογιστής με modem και η σύνδεση στο διαδίκτυο προκειμένου ο χρήστης να αποκτήσει πρόσβαση στις υπηρεσίες διαδικτυακής τραπεζικής (internet banking) των τραπεζών και όχι μόνο, και να δώσει εντολές πληρωμής on-line. Στην προσφορά υπηρεσιών τραπεζικής τηλεξυπηρέτησης μέσω τηλεφώνου (phone banking) έρχεται πλέον να προστεθεί και η διενέργεια πληρωμών μέσω κινητού τηλεφώνου (mobile banking) με αποστολή γραπτών μηνυμάτων και την τεχνολογία WAP (Wireless application protocol- πρωτόκολλο ασύρματης εφαρμογής).

# Δεύτερο μέρος

## 3. Νομικά ζητήματα σχετικά με το ηλεκτρονικό έγκλημα

### 3.1. Εισαγωγικά

Το ηλεκτρονικό έγκλημα είναι μια νέα μορφή εγκλήματος, που οριοθετείται από δύο βασικά στοιχεία: τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Η προσέγγιση των νομικών θεμάτων που αφορούν το ηλεκτρονικό έγκλημα ενέχει τη δυσκολία ότι προϋποθέτει όχι μόνο νομικές, αλλά και σε ένα βαθμό τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και Διαδικτύου. Τα προβλήματα της νομοθεσίας επικεντρώνονται στη διαμόρφωση της κατάλληλης ορολογίας, στην αρτιότερη εφαρμογή του Ποινικού και Δικονομικού Δικαίου, καθώς και σε ειδικότερα θέματα που άπτονται της διεθνούς συνεργασίας, όπως η διεθνής δικαιοδοσία.

Έως σήμερα, οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα προέρχονται κυρίως από την τεχνολογία. Ο τεχνικός, λόγω έλλειψης νομικών γνώσεων, προσδιορίζει τους όρους με βάση τις επιστημονικές του γνώσεις και τα τεχνολογικά χαρακτηριστικά κάθε αντικειμένου. Στη νομική επιστήμη, ο προσδιορισμός των όρων είναι τελείως διαφορετικός. Για το νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο που με ακρίβεια καθορίζει ο Νόμος. Σε περίπτωση που δεν υπάρχει νόμος ερευνάται η σχετική νομολογία και αν δεν υπάρχει ούτε νομολογία, η ανάλυση ανάγεται στους γενικούς κανόνες του ισχύοντος δικαίου για να βρεθεί κάποια θεωρητική λύση του ζητήματος.

Στην πράξη, ο νομοθέτης αποφεύγει να δημιουργήσει ειδική ορολογία για το ηλεκτρονικό έγκλημα και δανείζεται τη χρησιμοποιούμενη από την τεχνολογία, η οποία μπορεί να είναι ασαφής, γενική, αόριστη ή ελλιπής, κατά τρόπο που να εμποδίζει την ορθή απονομή της δικαιοσύνης.

Το ηλεκτρονικό έγκλημα φέρει κάποια ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα. Τα χαρακτηριστικά αυτά, απαιτούν την υιοθέτηση ειδικών νομοθετικών ρυθμίσεων για την αντιμετώπισή του, τόσο στον τομέα του Ποινικού, όσο και στον τομέα του Δικονομικού Δικαίου. Από άποψη Ποινικού Δικαίου, το ηλεκτρονικό έγκλημα σε πολλές χώρες αντιμετωπίζεται με τις υπάρχουσες διατάξεις του κοινού Ποινικού Δικαίου, γεγονός που πολλές φορές, καθιστά αδύνατη τη δίωξή του. Στον τομέα του

δικονομικού δικαίου, οι παρεμβάσεις στην ισχύουσα νομοθεσία παγκοσμίως, είναι ελάχιστες, με αποτέλεσμα να δημιουργούνται ανυπέρβλητα προβλήματα, όπως η δυσκολία ασφαλούς καθορισμού της δικαιοδοσίας των δικαστηρίων και της αρμοδιότητας των διωκτικών αρχών.

Με δεδομένο ότι η τεχνολογία προχωρά πολύ πιο γρήγορα από τη νομοθεσία, κάθε νομοθετική ρύθμιση υπόκειται πολύ γρήγορα σε αμφισβήτηση. Αυτό που σήμερα ορίζουμε ως ηλεκτρονικό έγκλημα, πολύ σύντομα δεν θα υπάρχει ως συμπεριφορά ή θα έχει τροποποιηθεί κατά τρόπο ουσιαστικό, που θα καθιστά ανίσχυρο τον υπάρχοντα νόμο.

Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν αρκεί μόνο ειδική νομοθεσία, αλλά απαιτείται συνεχής ενημέρωσή της, λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις. Επιπλέον, για ένα άρτιο σύστημα απονομής δικαιοσύνης, όλοι όσοι εμπλέκονται στη δίωξη του ηλεκτρονικού εγκλήματος όπως αστυνομικοί, εισαγγελείς, δικαστές και δικηγόροι, πρέπει να κατέχουν τόσο νομικές, όσο και τεχνικές γνώσεις, για τη νέα αυτή μορφή εγκληματικής δραστηριότητας.

Τέλος, τα σημαντικότερα νομοθετικά προβλήματα για το ηλεκτρονικό έγκλημα οφείλονται στον παγκόσμιο χαρακτήρα του. Ο τόπος διάπραξης των συμβατικών εγκλημάτων, προσδιορίζεται από έναν συγκεκριμένο γεωγραφικό χώρο. Στα ηλεκτρονικά εγκλήματα, ο τόπος διάπραξης πολλές φορές είναι αδύνατο να προσδιοριστεί, οι δε συνέπειες της εγκληματικής συμπεριφοράς, μπορούν να είναι ορατές σε περισσότερες από μία χώρες, στις οποίες ισχύει διαφορετικό νομοθετικό πλαίσιο. Η δικαιοδοσία, η συνεργασία μεταξύ των κρατών σε διεθνείς έρευνες ηλεκτρονικών εγκλημάτων και η διαδικασία έκδοσης όσων έχουν διαπράξει ηλεκτρονικά εγκλήματα με διεθνικό χαρακτήρα, είναι μερικά μόνο από τα ζητήματα που επιτείνουν τους νομοθετικούς προβληματισμούς.

## 3.2. Νομική προσέγγιση του διαδικτύου

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου, ενός «χώρου» τεράστιου και αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς,

που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου.[69]

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

- Το Διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του.
- Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.
- Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της.
- Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα:

✓ Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις.

✓ Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.

✓ Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας.

✓ Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχο τα κράτη με νομοθετικές ρυθμίσεις.

Το Διαδίκτυο, με άξονα τη βασική του χρήση ως μέσο επικοινωνίας, απασχόλησε τον νομοθέτη, ιδιαίτερα από το χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται.

---

[69] Ζάννη Αν. (2005) «*Το διαδικτυακό έγκλημα*», Εκδόσεις Σάκκουλα, Αθήνα

Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες (Καρακώστας, 2003). Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δύο Οδηγίες την 90/38794 και την 90/388;95 κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιονδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

Η προσαρμογή της ελληνικής νομοθεσίας προς τις παραπάνω οδηγίες της Ευρωπαϊκής Κοινότητας, προήλθε, κατ' αρχήν, με τον Ν. 2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Ν. 2246/94 και στη συνέχεια με τον Ν. 2867/2000, που ως σήμερα είναι σε ισχύ. Με τον νόμο αυτό, ιδρύθηκε ρυθμιστική αρχή[70], η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου[71].

## 3.3. Το ευρύτερο νομοθετικό πλαίσιο γύρω από το ηλεκτρονικό οικονομικό έγκλημα

Οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες, τόσο στην Ελλάδα όσο και σε άλλες χώρες. Με δεδομένο ότι η ψηφιακή εγκληματικότητα αποτελεί δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, παρουσιάζει προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος εκτός από τεχνικής απόψεως πρέπει να είναι και σύννομη, συμβαδίζοντας με τους ισχύοντες σε κάθε χώρα νόμους και κανονισμούς. Η Ηλεκτρονική Εγκληματολογία, ως μια σχετικά νέα επιστήμη, έχει προβληματίσει τους νομικούς κύκλους για το κατά πόσο αξιόπιστη είναι και σε ποιο βαθμό οι ψηφιακές αποδείξεις μπορούν να τύχουν εφαρμογής σε μια δίκη. Οι νομικοί προβληματισμοί σχετίζονται με την έρευνα και κατάσχεση (search and seizure) ψηφιακών αποδείξεων, το κατά

[70] Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους παρόχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους.

[71] Κ. Βλαχόπουλος, *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη, 2007

πόσο οι γνώσεις ενός ερευνητή είναι επαρκείς για τη διεκπεραίωση μιας έρευνας σε έναν Η/Υ και τέλος, αν η ανάλυση και διατήρηση των αποδείξεων έγινε σύμφωνα με τις προβλεπόμενες διαδικασίες.

Η έρευνα και κατάσχεση πληροφοριών είναι η πρώτη διαδικασία που αμφισβητείται σε μια δίκη. Σύμφωνα με το Ελληνικό Δίκαιο, μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακούργημα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να κατορθωθεί ή να διευκολυνθεί η βεβαίωση του εγκλήματος, η ανακάλυψη και σύλληψη των δραστών ή τέλος η βεβαίωση και αποκατάσταση της ζημιάς που προκλήθηκε. Επιπλέον, κατά τη διεξαγωγή μιας έρευνας θα πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπέρμετρου. Επειδή δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για τις διαδικτυακές έρευνες, οι ανωτέρω διατάξεις εφαρμόζονται κατά αναλογία και σε περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα στην οποία δεν έχουν τηρηθεί οι προβλεπόμενες προϋποθέσεις, θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχθηκαν. Κατά τη διεξαγωγή μιας έρευνας, το βασικό αγαθό, που διακυβεύεται, είναι η ιδιωτικότητα του ατόμου. Το Αμερικανικό Σύνταγμα απαιτεί την ύπαρξη εντάλματος για τη διεξαγωγή μιας έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αιτία (probable cause), ότι διαπράχθηκε ένα έγκλημα. Το ένταλμα θα πρέπει να καθορίζει, επακριβώς, το μέρος και τα αντικείμενα που μπορούν να ερευνηθούν. Για παράδειγμα, εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει στο χώρο για την εύρεση συμπληρωματικών στοιχείων. Αν το πράξει, έστω και αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο, γιατί παραβιάστηκε το ένταλμα. Ταυτόχρονα ζήτημα αφορά η ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξετασθεί (π.χ. ενός σκληρού δίσκου) δημιουργώντας ακριβές αντίγραφο. Τα δικαστήρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο. Ωστόσο, πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την άρτια διατήρησή του.

Οι ψηφιακές πληροφορίες μπορούν να επηρεαστούν από μαγνητικά πεδία, καιρικές συνθήκες κ.ά. Για παράδειγμα, στη υπόθεση Ohio v. Cook[72], ο κατηγορούμενος προέβαλλε

[72] Βλ. *Ohio v. Cook*, 149 Ohio App. 3d 422 (2d App.Dist. 2002)

μια σειρά από ισχυρισμούς έναντι της μη ορθής συλλογής και διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωσή τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θέση. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά τη διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών[73].

Το δεύτερο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχεία σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για τη διεκπεραίωση μιας ηλεκτρονικής έρευνας. Ο μεγαλύτερος προβληματισμός έγκειται στα χρησιμοποιούμενα από τον ερευνητή εργαλεία λογισμικού. Ο ερευνητής, απλά, γνωρίζει τη χρήση ενός εργαλείου λογισμικού. Δεν μπορεί να έχει πρόσβαση στον πηγαίο κώδικα και έτσι δεν γνωρίζει τι εργασίες επιτελεί το λογισμικό. Πώς λοιπόν μπορεί να βεβαιώσει ότι τα ψηφιακά δεδομένα, που συλλέχθηκαν, αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορουμένου; Έως σήμερα, δεν υπάρχει απόφαση δικαστηρίου που να απέρριψε την επιστημονική άποψη ενός ερευνητή, τέτοιο ενδεχόμενο, όμως, δεν αποκλείεται να συμβεί στο μέλλον από τη στιγμή που τα εργαλεία λογισμικού εξελίσσονται με ραγδαίους ρυθμούς και γίνονται όλο και πιο πολύπλοκα. Το τρίτο και τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξεταστεί, (π.χ. ενός σκληρού δίσκου) δημιουργώντας ένα ακριβές αντίγραφο (bit-stream image), του πρωτοτύπου. Τα δικαστήρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο.

Επιπλέον ο νομοθέτης είναι αναγκασμένος να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθεί με τον τρόπο διάπραξης των σχετικών αξιόποινων πράξεων. Οι διώξεις των ψηφιακών εγκλημάτων κινούνται σε χαμηλά επίπεδα, εφόσον και οι καταγγελίες είναι περιορισμένες. Γενικά, θα πρέπει να παρατηρήσουμε πως οι επιχειρήσεις – κυρίως - αποφεύγουν να καταγγείλουν παραβάσεις, γιατί φοβούνται επανάληψη των αδικημάτων και πλήγμα στη φήμη τους. Επίσης, θέλουν να αποφεύγουν τα υψηλά δικαστικά έξοδα και το γεγονός ότι δεν γίνεται εύκολη χρηματική και αξιακή αποτίμηση των οικονομικών ζημιών που τελικά υφίστανται. Οι δυσκολίες που αντιμετωπίζουν οι αστυνομικές και οι δικαστικές αρχές στον εντοπισμό και

[73] Βλαχόπουλος Κ. (2007) όπ. παρ. σελ. 182, 183

την περαιτέρω δίωξη, σχετίζονται, κυρίως, με το συνήθως, χαμηλό επίπεδο πληροφορικής κατάρτισης των στελεχών τους.

Επίσης απαιτείται συνήθως αρκετός χρόνος, για να διευκρινιστούν οι υποθέσεις, που είναι συνήθως πολύπλοκες και απαιτούν συνεργασία και με άλλες υπηρεσίες. Πολλές φορές οι δικαστές υποβαθμίζουν τη σημασία των ψηφιακών εγκλημάτων, με τη δικαιολογία ότι το σύστημα της ποινικής δικαιοσύνης δεν θα πρέπει να επιβαρυνθεί με τέτοιου είδους εγκληματίες, εφόσον η ποινή που τους επιβάλλεται, δεν είναι ικανή να τους αποτρέψει από την επανάληψη της πράξης. Ο διεθνής εξάλλου χαρακτήρας του συγκεκριμένων εγκλημάτων δίνει τη δυνατότητα στους δράστες να έχουν γρήγορη πρόσβαση στα στοιχεία, αλλά και εύκολη προσβολή των δεδομένων στα συστήματα Η/Υ παγκοσμίως. Βασικό στοιχείο που εμποδίζει την διωκτική προσπάθεια είναι η διασύνδεση των πιο επικίνδυνων από τους ψηφιακούς εγκληματίες με το οργανωμένο έγκλημα. Θα πρέπει επιπρόσθετα να σημειώσουμε πως τα ψηφιακά εγκλήματα διακρίνονται και για: το μεγάλο όγκο των δεδομένων τους, τον μη οπτικό χαρακτήρα των αποδείξεων, τη δυνατότητα «μεταμφίεσης» τους καθώς και την ταχεία εξαφάνιση των αποδεικτικών στοιχείων από τη μεριά των εγκληματιών.

Ο τεράστιος αριθμός δεδομένων που είναι καταχωρημένα στο Διαδίκτυο και η παγκοσμιότητά του αποτελούν εμπόδιο στην αντιμετώπιση αξιόποινων πράξεων που διαπράττονται σε αυτό. Επιπλέον, υπάρχει το πρόβλημα της δικαιοδοσίας, αφού ο καθένας όπου και αν βρίσκεται μπορεί να έχει πρόσβαση σε οποιαδήποτε πληροφορία θελήσει. Είναι δύσκολο να ορισθεί ο τόπος τέλεσης του αδικήματος και η αρμοδιότητα του δικαστηρίου που θα πρέπει να εκδικάσει την υπόθεση. Στην Ελλάδα και την Ευρώπη κυριαρχεί η θεωρία του βαρύνοντος τόπου, δηλαδή ο τόπος του αδικήματος εντοπίζεται στο κράτος που εκδηλώθηκε το έγκλημα. Και σε αυτό όμως, παρουσιάζονται προβλήματα, εφόσον είναι δύσκολο να καθοριστεί ο τόπος τέλεσης ενός διαδικτυακού αδικήματος. Με δεδομένη όμως, την αύξηση των μορφών και του αριθμού των ψηφιακών εγκλημάτων[74] η ειδική και εξειδικευμένη νομοθετική αντιμετώπισή τους θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν όλα τα κράτη του κόσμου έχουν θεσπίσει νομοθετικές διατάξεις, σχετικές με τα ψηφιακά εγκλήματα. Ωστόσο, το νομοθετικό πλαίσιο που να αφορά ειδικότερα το ζήτημα είναι, όπως θα φανεί και

[74] Βλ. σχετικά. *Ν. Κουράκης,* Το οικονομικό έγκλημα στην Ελλάδα σήμερα σε: *του ιδίου* Εγκληματολογικοί ορίζοντες Β΄, 2005, σελ. 163 επ., 183.

παρακάτω, σε αρκετές περιπτώσεις εξαιρετικά ελλιπές και συνήθως καλύπτεται από γενικότερες διατάξεις.

Τα τελευταία χρόνια έχουν πραγματοποιηθεί Συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως, με σκοπό τη συζήτηση και τη λήψη αποφάσεων, σχετικά με το ζήτημα αυτό.

Στην Ελλάδα, όπως θα εξετάσουμε και παρακάτω, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές.[75]

## 3.4. Ο ρόλος και οι επιδιώξεις του νομοθέτη στο ζήτημα

### 3.4.1. Τόπος τελέσεως του αδικήματος και το αρμόδιο δικαστήριο

❖ *Δικαιοδοσία στο Ίντερνετ*

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος.

Το έγκλημα εκτός από τη λεγόμενη αντικειμενική υπόσταση (δηλ. την περιγραφή των πράξεων που συνιστούν κολάσιμη συμπεριφορά) προσδιορίζεται από α) τον χρόνο τέλεσης, β) τον τόπο τέλεσης και γ) τα εμπλεκόμενα πρόσωπα (θύμα, παραβάτης κλπ.).

Ο προσδιορισμός του τόπου τέλεσης του (διαδικτυακού) εγκλήματος έχει κρίσιμη σημασία καθώς από αυτόν εξαρτάται καταρχήν ο προσδιορισμός του εφαρμοστέου δικαίου και τα αρμόδια δικαστήρια. Εν γένει ο προσδιορισμός του τόπου εξαρτάται κατά περίπτωση από τον τόπο εκδήλωσης της αξιόποινης συμπεριφοράς και τον τόπο επέλευσης των αποτελεσμάτων της.

---

[75] Συγκεκριμένα με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα 370Β, 370Γ και 386Α.

«Τόπος» τέλεσης των ηλεκτρονικών εγκλημάτων είναι ο αποκαλούμενος κυβερνοχώρος, ο οποίος σύμφωνα με το «λεξικό διαδικτύου και δικτύων της Microsoft», προσδιορίζεται ως εξής: « το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση». Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε. Ως τόπος τελέσεως ενός εγκλήματος θεωρείται από τις περισσότερες έννομες τάξεις (στις οποίες συμπεριλαμβάνεται και η ελληνική) τόσο ο τόπος στον οποίο ο υπαίτιος προέβη, ολικά ή εν μέρει, στην αξιόποινη ενέργεια/παράλειψη όσο και ο τόπος, στον οποίο επήλθε το λεγόμενο αξιόποινο αποτέλεσμα. Η χρήση των υπολογιστών και το Διαδίκτυο δημιουργούν εντελώς νέα δεδομένα σχετικά με τον προσδιορισμό του τόπου καθώς είτε δεν είναι ευχερής ο προσδιορισμός του τόπου εκδήλωσης μιας συμπεριφοράς/επέλευσης ενός αποτελέσματος είτε συντρέχουν περισσότεροι τόποι όπου τελείται ένα έγκλημα Στην περίπτωση εγκλημάτων που τελούνται/εκδηλώνονται στο Διαδίκτυο ο τόπος επέλευσης είναι ο κυβερνοχώρος[76], ο οποίος θα μπορούσε να ερμηνευτεί ως «κάθε χώρος στον οποίο αποκτάται πρόσβαση στα δεδομένα, δηλ. παντού»

Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα. Ως τόπος επελεύσεως του αποτελέσματος στην πραγματικότητα μπορεί να θεωρηθεί το Διαδίκτυο, κάθε χώρος δηλαδή στον οποίο αποκτάται πρόσβαση στα δεδομένα. Ο τόπος του κυβερνοεγκλήματος είναι

[76] Ως ψηφιακός τόπος τελέσεως του εγκλήματος μπορεί να θεωρηθεί το εικονικό περιβάλλον που δημιουργείται από το λογισμικό και το υλικό στα οποία υπάρχουν τα ψηφιακά στοιχεία ενός εγκλήματος και τα οποία παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του θύματός του ή μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του δράστη του. Λόγω της φύσης του Διαδικτύου είναι πολύ δύσκολο να εντοπιστεί τόσο ο τόπος στον οποίο εκδηλώθηκε η συμπεριφορά του εγκληματία όσο και ο τόπος στον οποίο επήλθε το αξιόποινο αποτέλεσμα. Ενδέχεται μάλιστα να υπάρχουν περιπτώσεις με περισσότερους τόπους τέλεσης της εγκληματικής πράξης [IRC (Internet Relay Channel), τα newsgroups (ομάδες συζητήσεως), το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol) κλπ.] βλ.σχετικά, Δ. Κιούπη, Ποινικό Δίκαιο και Internet, 1999, εκδόσεις Αντ. Σάκκουλα σελ. 145-176.

διαφορετικός από τον τόπο του εγκλήματος στον «φυσικό» κόσμο δεδομένου ότι ο τόπος του κυβερνοεγκλήματος είναι δυναμικός, αυξάνεται και μπορεί να μεταμορφωθεί.

Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Ο M. Collardin προτείνει μία άλλη θεωρία, σύμφωνα με την οποία πρέπει να περιλαμβάνεται και ο τόπος που επήλθε το αξιόποινο αποτέλεσμα υπό την προϋπόθεση να καλύπτεται από τη γνώση και τον δόλο του δράστη[77]. Είναι γεγονός ότι στις διαδικτυακές πράξεις υπάρχει πάντα ο δόλος του δράστη. Η πιθανότητα, οι περιορισμοί των τόπων τέλεσης της εγκληματικής πράξης να γίνονται περισσότεροι και ακριβέστεροι υπάρχει στους τόπους εκείνους στους οποίους ο δράστης ενήργησε με δόλο πρώτου βαθμού δηλαδή σε εκείνους τους τόπους που ο δράστης είχε σκοπό να επέλθει το αποτέλεσμα.

Μια άλλη λύση που αναπτύχθηκε για να προσδιοριστεί ο τόπος τέλεσης μιας παράνομης ενέργειας είναι ο διαχωρισμός των εγκλημάτων σε διάφορες κατηγορίες. Παραδείγματος χάριν στα τυπικά εγκλήματα ή όπως αλλιώς λέγονται εγκλήματα συμπεριφοράς, αποφασιστικός είναι ο τόπος που εκδηλώθηκε η συμπεριφορά του δράστη, δηλαδή ο τόπος που ο υπαίτιος διέπραξε την αξιόποινη πράξη και όχι ο τόπος που κατά τύχη επήλθε ο κίνδυνος. Φυσικά η λύση αυτή δεν είναι και τόσο εύκολο να επιτευχθεί για το λόγο ότι είναι αρκετά δύσκολο να διαχωριστούν τα εγκλήματα συμπεριφοράς με τα εγκλήματα αποτελέσματος καθώς επίσης τα εγκλήματα συγκεκριμένης διακινδυνεύσεως με τα εγκλήματα αφηρημένης διακινδυνεύσεως.

Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς

---

[77] M. Collardin, Straftaeten im Internet, CR 1995, σελ. 620, Schlmer/Conradi, Die Strafbarkeit der Internet Provider}, NStZ 1996, σελ. 369

εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα.

### 3.4.2. Ο τόπος του ηλεκτρονικού εγκλήματος στο ελληνικό δίκαιο

Σύμφωνα με το άρθρο 16 του Ποινικού Κώδικα «τόπος τέλεσης της πράξης θεωρείται ο τόπος που ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη καθώς και ο τόπος που επήλθε, ή σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει το αξιόποινο αποτέλεσμα».

Το άρθρο 16 Ποινικού Κώδικα διατυπώθηκε και τέθηκε σε εφαρμογή πολύ πριν ανακαλυφτεί το Διαδίκτυο γι' αυτό το λόγο θα πρέπει να επιτευχθεί μια σύνδεση μεταξύ του Κυβερνοχώρου και του φυσικού χώρου. Όπως επισημάνθηκε ήδη το πρόβλημα που προκύπτει εδώ είναι ότι μπορεί να υφίστανται περισσότεροι από ένας τόποι εγκλήματος αφού σαν τόπο που πραγματοποιήθηκε το έγκλημα έχουμε και τον τόπο συμπεριφοράς του παραβάτη και τον τόπο του αξιόποινου αποτελέσματος.

Στην Ελλάδα και γενικότερα στην Ευρώπη κρατούσα θεωρία είναι η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία «ο τόπος του αδικήματος εντοπίζεται στο κράτος που εκδηλώθηκε το έγκλημα κατά την κύρια σημασία του». Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας αυτής δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Όσον αφορά το ελληνικό ποινικό δίκαιο, αυτό ενδιαφέρεται για τον τόπο του εγκλήματος ως στοιχείο της αξιόποινης πράξης και όχι ως φυσικό δεδομένο. Από αυτό βγαίνει το συμπέρασμα ότι στην συγκεκριμένη περίπτωση ο τόπος του εγκλήματος δεν ακολουθεί την φυσική έννοια του τόπου. Επιπλέον ο τόπος αποτελεί κριτήριο εφαρμογής των ελληνικών ποινικών νόμων και άσκησης της ελληνικής ποινικής δικαιοδοσίας.

Πιο συγκεκριμένα για τα εγκλήματα που εμπίπτουν στο άρθρο 8 του Ποινικού Κώδικα το πρόβλημα του τόπου τέλεσης δεν έχει πρακτικά σημασία αφού εφαρμόζονται οι ελληνικοί ποινικοί νόμοι ανεξαρτήτως τόπου τελέσεως. Το άρθρο 8 Ποινικού Κώδικα αφορά τα εγκλήματα στην αλλοδαπή που τιμωρούνται πάντοτε κατά τους ελληνικούς νόμους. Σύμφωνα

με το άρθρο αυτό οι ελληνικοί ποινικοί νόμοι εφαρμόζονται σε ημεδαπούς κι αλλοδαπούς ανεξάρτητα από τους νόμους του τόπου της τέλεσης, για τις εξής πράξεις που τελέστηκαν στην αλλοδαπή: α) έσχατη προδοσία και προδοσία της χώρας που στρέφεται κατά του ελληνικού κράτους. β) εγκλήματα που αφορούν τη στρατιωτική υπηρεσία και την υποχρέωση στράτευσης γ) η αξιόποινη πράξη που τέλεσαν ως υπάλληλοι του ελληνικού κράτους. δ) πράξη εναντίον Έλληνα υπαλλήλου κατά την άσκηση της υπηρεσίας του ή σχετικά με την υπηρεσία του. ε) ψευδορκία σε διαδικασία που εκκρεμεί στις ελληνικές αρχές. στ) πειρατεία. ζ) εγκλήματα σχετικά με το νόμισμα η) πράξη δουλεμπορίου ή σωματεμπορίας με σκοπό την ακολασία. θ) παράνομο εμπόριο ναρκωτικών φαρμάκων. ι) παράνομη κυκλοφορία και εμπόριο άσεμνων δημοσιευμάτων. κ) κάθε άλλο έγκλημα, για το οποίο ειδικές διατάξεις ή διεθνείς συμβάσεις υπογραμμένες και επικυρωμένες από το ελληνικό κράτος προβλέπουν την εφαρμογή των ελληνικών ποινικών νόμων.

Στην περίπτωση των εγκλημάτων αποτελέσματος ή συγκεκριμένης διακινδύνευσης αν ο κίνδυνος ή το αποτέλεσμα επήλθαν στην Ελλάδα εφαρμόζεται το δίκαιο της ημεδαπής[78]. Το άρθρο αυτό αφορά τα εγκλήματα που τελέστηκαν στην ημεδαπή και τονίζει ότι οι ελληνικοί ποινικοί νόμοι εφαρμόζονται σε όλες τις πράξεις που τελέστηκαν στο έδαφος της επικρατείας, ακόμη και από αλλοδαπούς.

Στην περίπτωση των παραπάνω εγκλημάτων αλλά και των εγκλημάτων συμπεριφοράς και αφηρημένης διακινδύνευσης εφαρμόζεται το ελληνικό ποινικό δίκαιο αν ο δράστης διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια στην Ελλάδα.

[78] Βλ. άρθρο 5 ΠΚ

## 4. Το διεθνές δίκαιο

### 4.1. Οι πρώτες συνεργασίες σε διεθνές επίπεδο

Σε διεθνές επίπεδο, η Interpol[79] προσέγγισε πρώτη το ζήτημα του ηλεκτρονικού εγκλήματος, στο Τρίτο Διεθνές Συμπόσιο για την Απάτη, στο Παρίσι, το 1979[80]. Διάφορες άλλες προσεγγίσεις έλαβαν χώρα κατά τα χρόνια που ακολούθησαν, με πιο σημαντικές αυτές που αναπτύχθηκαν από τον OECD, τα Ηνωμένα Έθνη και την «Ομάδα των Οκτώ». Όπως είναι φυσικό κάθε χώρα μεμονωμένα είναι σε θέση να αναπτύσσει την δική της άμυνα απέναντι στις υποθέσεις του ηλεκτρονικού οικονομικού εγκλήματος και να θεσπίζει το δικό της νομικό πλαίσιο. Στην Μ. Βρετανία από τον Φεβρουάριο του 2001 οι hackers, αναλόγως με τη σημασία του «χτυπήματος» μπορούν να θεωρηθούν και να κατηγορηθούν ως τρομοκράτες. Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της «εισβολής»), χωρίς δυνατότητα εξαγοράς ή μείωσης της ποινής.

α) Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α)

Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη διόρισε στο Παρίσι, το 1983, μια επιτροπή, για το ζήτημα του ηλεκτρονικού εγκλήματος και την ανάγκη, που αυτό δημιουργεί, για την τροποποίηση των ποινικών διατάξεων στα κράτη-μέλη του οργανισμού. Η επιτροπή, αφού εξέτασε τις ισχύουσες νομοθετικές διατάξεις των κρατών-μελών, κατέληξε σε ένα κείμενο για το ηλεκτρονικό έγκλημα, που λειτουργούσε ως κοινός παρονομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη-μέλη.

Σύμφωνα με τον ΟΟΣΑ η εγκληματικότητα μέσω των υπολογιστών "αφορά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και μεταφορά στοιχείων"

---

[79] Με την διεθνή ονομασία Ιντερπόλ της οποίας το πλήρες όνομα είναι International Criminal Police Organization (ICPO) – INTERPOL, *Διεθνής Οργάνωση Εγκληματολογικής Αστυνομίας*, φέρεται σήμερα ένας σπουδαίος διακυβερνητικός οργανισμός, μη κυβερνητικός, ο μεγαλύτερος σε παγκόσμια κλίμακα μετά τον ΟΗΕ Σκοπός της σύστασης αυτού του οργανισμού είναι κυρίως η προώθηση της αμοιβαίας συνεργασίας των διαφόρων «εθνικών» αστυνομικών Αρχών των Χωρών –μελών που τον απαρτίζουν προκειμένου η πρόληψη της εγκληματικότητας να είναι περισσότερο αποτελεσματική σε παγκόσμιο επίπεδο. Η Ιντερπόλ χρηματοδοτείται από τις 187 Χώρες μέλη της. Το 1997 ο προϋπολογισμός της έφθανε τα 27 εκατομμύρια δολάρια, ενώ το 2008 ξεπέρασε τα 47 εκατομμύρια δολλάρια.

[80] Κ. Βλαχόπουλος, *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη, 2007, σελ.133-135

Οι διατάξεις του κειμένου αυτού απαγόρευαν την εισαγωγή, τροποποίηση, διαγραφή και απόκρυψη δεδομένων, με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτύου. Επίσης, απαγόρευαν την πρόσβαση σε σύστημα Η/Υ χωρίς άδεια, ενώ προστάτευαν και την παράνομη αντιγραφή και διάθεση πακέτων λογισμικού.

β) Ο Οργανισμός Ηνωμένων Εθνών

Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα, σχετικά με τη νομοθεσία για το ηλεκτρο-νικό έγκλημα, στο 8° Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994. Το Εγχειρίδιο αυτό αντιμετωπίζει συνολικά το ζήτημα του ηλεκτρονικού εγκλήματος παρουσιάζοντας την έκταση του φαινομένου, τις μορφές του και την υπάρχουσα νομοθεσία σε διάφορες χώρες, και καταλήγει σε προτάσεις για την καλύτερη αντιμετώπισή του.

Το συγκεκριμένο κείμενο έχει υποστεί αναθεωρήσεις λόγω των τεχνολογικών εξελίξεων που συντελέστηκαν μετά την έκδοση του. Αποτελεί, όμως, την πρώτη συστηματική διεθνή προσπάθεια νομοθετικής προσέγγισης του ηλεκτρονικού εγκλήματος. Για το λόγο αυτό, θεωρείται η βάση πάνω στην οποία μπορούν να στηριχθούν μελλοντικές προσπάθειες.

Στα πλαίσια της συνόδου κορυφής για την κοινωνία της πληροφορίας του ΟΗΕ που πραγματοποιήθηκε το Νοέμβριο του 2005 στην Τύνιδα καθιερώθηκε το Forum Διακυβέρνησης Διαδικτύου (Internet Governance Forum, IGF[81]) του ΟΗΕ.

Το Forum Διακυβέρνησης Διαδικτύου είναι μια ετήσια συνάντηση[82], που διοργανώνεται σε διαφορετικές χώρες[83] και είναι ανοιχτό στη συμμετοχή των κυβερνήσεων, του ιδιωτικού τομέα και της κοινωνίας των πολιτών ενώ πρέπει να σημειωθεί ότι το IGF δεν είναι ένα όργανο λήψης αποφάσεων, αλλά έχει συσταθεί ως ένα forum διαλόγου για πολιτικές με ισχυρές αξιώσεις πολυμερούς εμπλοκής και συμμετοχής.

[81] http://www.intgovforum.org/cms/

[82] Η Εναρκτήρια Συνάντηση του IGF έγινε στην Αθήνα, από τις 30 Οκτωβρίου - 2 Νοεμβρίου 2006.

[83] Ελλάδα 2006, Βραζιλία 2007, Ινδία 2008, Αίγυπτος 2009, Λιθουανία 2010

## 4.2. Αρμόδιες υπηρεσίες για το έγκλημα στον Κυβερνοχώρο διεθνώς

Στα λεγόμενα τεχνολογικώς αναπτυγμένα κράτη, όπου το έγκλημα στον κυβερνοχώρο ``ανθεί``, έχουν συσταθεί ειδικές υπηρεσίες για την έρευνα και καταπολέμηση του νέου αυτού εγκλήματος. Ενδεικτικώς αναφέρεται ότι στις Η.Π.Α. το F.B.I. έχει συστήσει το National Infrastructure Protection Center (NIPC), με παραρτήματα σε διάφορες πολιτείες για την έρευνα των σχετικών εγκλημάτων. Στα πλαίσια μάλιστα της ``Ηλεκτρονικής Αστυνομίας`` έχει συσταθεί ειδική μονάδα, που έχει ως αντικείμενο το ``σπάσιμο`` των κωδικών των ηλεκτρονικών επιστολών (e-mails ), που χρησιμοποιούν οι έμποροι ναρκωτικών και τα δίκτυα παιδεραστίας . Ομοίως έχει συσταθεί ειδικό σώμα Εισαγγελέων, οι οποίοι ύστερα από κατάλληλη εκπαίδευση, ασχολούνται με το έγκλημα στον κυβερνοχώρο . Παρόμοια εκπαίδευση έχει γίνει και στους Δικαστές. Στην Scotland Yard έχει συσταθεί το Computer Fraud Squad. Στον Καναδά έχει συσταθεί το the Royal Canadian Mounted Police Computer Crime Unit.

Δεκάδες συναντήσεις, συνέδρια κλπ γίνονται κάθε χρόνο από τις παραπάνω υπηρεσίες για θέματα σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Επίσης έχουν εκδοθεί δεκάδες γραπτές οδηγίες (guide lines) και Κώδικες Πρακτικής (Code of Practice), που απευθύνονται στους δημόσιους εκείνους λειτουργούς, οι οποίοι είναι επιφορτισμένοι με την έρευνα και την καταπολέμηση των σχετικών εγκλημάτων. Ενδεικτικώς αναφέρεται ο Κώδικας Πρακτικής του Τμήματος Εμπορίου και Βιομηχανίας (DTI) της Βρετανίας (The British Code of Practice - Department of Industry).

## 4.3. Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο που πραγματοποιήθηκε στη Βουδαπέστη στις 23 Νοεμβρίου 2001

### 4.3.1. Γενικά

Το Συμβούλιο της Ευρώπης έχει ασχοληθεί τόσο με το ηλεκτρονικό έγκλημα όσο και με το έγκλημα στον Κυβερνοχώρο. Στη συνέχεια δύο – μη νομικά δεσμευτικών – συστάσεων (Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή[84]

[84] Βλ. σχετικά Τάσου Ν. Μαρίνου, Σύμβουλου Επικρατείας, Οι ηλεκτρονικοί υπολογιστές και το Δίκαιο, εκδ. Σάκκουλα 1991, σελ. 144.

και Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών ) ιδιαίτερα σημαντική εξέλιξη υπήρξε η σύναψη **διεθνούς Σύμβασης** στο πλαίσιο του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο. Συγκεκριμένα στις 23 Νοεμβρίου 2001 στη Βουδαπέστη υπογράφηκε η πρώτη διεθνής σύμβαση «για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο» και «άνοιξε» προς υπογραφή και υπογράφτηκε από τριάντα χώρες τότε (από 26 μέλη του Ευρωπαϊκού Συμβουλίου και 4 χώρες μη μέλη[85] που συμμετείχαν, όμως, στο σχεδιασμό της συνθήκης). Το δεσμευτικό αυτό κείμενο μπορούν να υπογράφουν και άλλες χώρες που δεν είναι μέλη του Συμβουλίου της Ευρώπης, μετά από πρόσκληση της Επιτροπής Υπουργών. Μεταξύ των χωρών που υπόγραψαν την συνθήκη ήταν και η Ελλάδα.

Η συνθήκη τέθηκε σε ισχύ από τη στιγμή που επικυρώθηκε από πέντε κράτη, τουλάχιστον τρία από τα οποία είναι μέλη του Συμβουλίου της Ευρώπης.

4.3.2. Σκοποί της Σύμβασης είναι:

α) Η εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών μελών στον τομέα της εγκληματικότητας στον Κυβερνοχώρο.

β) Η θέσπιση εσωτερικών δικονομικών ποινικών διατάξεων, που είναι απαραίτητες για την έρευνα, δίωξη και εκδίκαση των εγκλημάτων του Κυβερνοχώρου, καθώς και των άλλων εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών, αλλά και για τη συλλογή αποδεικτικών στοιχείων, που βρίσκονται σε ηλεκτρονική μορφή.

γ) Η θέσπιση γρήγορων και αποτελεσματικών κανόνων στον τομέα της διεθνούς συνεργασίας και επικοινωνίας.

4.3.3. Η Σύμβαση περιέχει:

α) Διατάξεις ουσιαστικού ποινικού δικαίου. Συγκεκριμένα περιέχει ρυθμίσεις για τα ακόλουθα:

[85] Καναδάς, Ιαπωνία, Ν. Αφρική και ΗΠΑ

i. Αδικήματα που αφορούν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που έχουν αποθηκευτεί σε υπολογιστικά συστήματα και των συστημάτων Η/Υ. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η αθέμιτη παγίδευση - υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

ii. Αδικήματα που διαπράττονται με τη χρήση υπολογιστών όπως η απάτη με η/υ και πλαστογραφία.

iii. Αδικήματα σχετικά με το περιεχόμενο όπως είναι η κατοχή και διεθνής διανομή υλικού παιδικής πορνογραφίας.

iv. Αδικήματα που αποτελούν παραβίαση της πνευματικής ιδιοκτησίας και των σχετικών δικαιωμάτων.

β) Διατάξεις ποινικού δικονομικού δικαίου.

Οι διατάξεις ποινικού δικονομικού δικαίου αναφέρονται σε θέματα:

1. Ταχείας διαφύλαξης δεδομένων αποθηκευμένων σε σύστημα υπολογιστή (Expedited preservation of stored computer data).
2. Ταχείας διαφύλαξης και γνωστοποίησης διακινουμένων δεδομένων (Expedited preservation and disclosure of traffic data).
3. Εντολής παροχής πληροφοριών (Production order).
4. Έρευνας και κατάσχεσης αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή (Search and Seizure of stored Computer data).
5. πραγματικού χρόνου συλλογής διακινουμένων δεδομένων (Real time collection of traffic data).
6. Παγίδευσης - υποκλοπής περιεχομένου δεδομένων (Interception of content data).

γ) Διατάξεις διεθνούς δικαστικής συνεργασίας. Οι διατάξεις διεθνούς δικαστικής συνεργασίας αναφέρονται:

1) Στην έκδοση.

2) Σε γενικές αρχές σχετικές με την αμοιβαία συνδρομή.

3) Σε παροχή αυθόρμητων πληροφοριών.

4) Στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών (Expedited preservation of stored computer data).

5) Στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων (Expedited disclosure of preserved traffic data).

Η Σύμβαση περιέχει επίσης ρυθμίσεις για την συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων ενώ υπογραμμίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και τίθεται το ιδιαίτερα σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά.

Η Σύμβαση εισάγει την υποχρέωση εναρμόνισης των εθνικών νομοθεσιών σε θέματα εγκλημάτων στον Κυβερνοχώρο σε θέματα τόσο ποινικού όσο και αστικού Δικαίου. Κύριο χαρακτηριστικό της Σύμβασης είναι η υποχρέωση που αναλαμβάνουν τα κράτη μέλη να ποινικοποιήσουν ορισμένη συμπεριφορά στο Διαδίκτυο, όπως είναι η διανομή πορνογραφικού υλικού στο Διαδίκτυο, η «εμπλοκή ανηλίκου σε ερωτική επαφή» με τη χρήση του Διαδικτύου, η αντιγραφή (χωρίς δικαίωμα) έργων πνευματικής ιδιοκτησίας.

### 4.3.4. Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών.

#### 4.3.4.1. Παράνομη πρόσβαση (Illegal Access)

Σύμφωνα με το άρθρο 2 της Σύμβασης κάθε μέλος θα θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα και με δόλο. Το μέρος μπορεί να απαιτεί ότι το αδίκημα θα διαπράττεται ή με παραβίαση των μέτρων ασφαλείας ή με σκοπό απόκτησης ηλεκτρονικών δεδομένων ή για άλλο παράνομο σκοπό ή σε σχέση με ένα σύστημα ηλεκτρονικών υπολογιστών, που συνδέεται με άλλο σύστημα ηλεκτρονικών υπολογιστών.

Το άρθρο αυτό έχει ως στόχο να ποινικοποιήσει το «computer hacking». Ο δικαιολογητικός λόγος της ποινικοποίησης της παράνομης πρόσβασης συνίσταται στο γεγονός ότι ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσης του υπολογιστή ή του συστήματος υπολογιστή.

Ο όρος «πρόσβαση» περιλαμβάνει τη «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή μέρος αυτού (π.χ. σε επιμέρους φακέλους). Δεν περιλαμβάνει όμως τη χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων.

Για τη θεμελίωση της υποκειμενικής υπόστασης απαιτείται πρόθεση, όπως αυτή προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε κράτους μέλους. Οι περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή.

4.3.4.2. Αθέμιτη παγίδευση- Υποκλοπή (illegal interception)

Σύμφωνα με το άρθρο 3[86] της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η παγίδευση – υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία. Ένα μέλος μπορεί να απαιτήσει ότι το αδίκημα διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών, το οποίο συνδέεται με άλλο σύστημα.

Η διάταξη αυτή εφαρμόζεται σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων είτε αυτά διακινούνται δια του Κυβερνοχώρου με μεταφορά φακέλων (file transfer) είτε με e-mail

[86] Στην περίπτωση της αθέμιτης πρόσβασης σε διαβιβαζόμενα δεδομένα που μεταδίδονται με συστήματα επικοινωνιών δεν εφαρμόζεται πλέον στη χώρα μας η διάταξη του άρθρου 370Γ παρ.2 Π.Κ., αλλά η νεότερη διάταξη του άρθρου 10 Ν. 3115/2003 («Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από δεκαπέντε χιλιάδες (15.000) έως εξήντα χιλιάδες (60.000) ευρώ, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις..»)

είτε με FAX. Προστατευόμενο έννομο αγαθό [87]είναι το δικαίωμα στην ιδιωτική ζωή και την ασφάλεια των τηλεπικοινωνιών στον Κυβερνοχώρο. Αποτελεί, δηλαδή, το άρθρο αυτό το «ηλεκτρονικό αντίστοιχο στον Κυβερνοχώρο» της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας (υποκλοπή).

4.3.4.3. Επέμβαση σε δεδομένα (Data interference)

Σύμφωνα με το άρθρο 4 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττονται εκ προθέσεως η καταστροφή (damaging), η διαγραφή (deletion), η χειροτέρευση (deterioration), η μεταβολή (alteration), ή η απόκρυψη (suppression) δεδομένων χωρίς δικαίωμα.

Σκοπός του άρθρου αυτού είναι να προστατεύσει τα δεδομένα (data) και τα προγράμματα των ηλεκτρονικών υπολογιστών ως «υλικές υποστάσεις» από οποιαδήποτε επέμβαση (παρεμβολή), που γίνεται με πρόθεση πρόκλησης ζημιάς σ΄αυτά. Προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

4.3.4.4. Επέμβαση σε σύστημα (System Interference)

Σύμφωνα με το άρθρο 5 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, για να καθιερωθεί ως ποινικό αδίκημα, σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττεται εκ προθέσεως, η σοβαρή παρεμπόδιση, χωρίς δικαίωμα και με δόλο, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με εισαγωγή (inputting), μεταφορά (transmitting), καταστροφή (damaging), διαγραφή (deleting), χειροτέρευση (deterioration), μεταβολή (alteration) ή απόκρυψη (suppression) δεδομένων υπολογιστών. Το προστατευόμενο έννομο αγαθό στο άρθρο αυτό είναι το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του. Η διάταξη αυτή ποινικοποιεί

[87] Η πρόσληψη της εννοίας του εννόμου αγαθού ως αντικειμένου προστασίας του ποινικού δικαίου, συνδέεται όπως είναι γνωστό με τη γερμανική παράδοση και συνιστά μία από τις πιο σημαντικές παρακαταθήκες της γερμανικής ποινικής επιστήμης στον ευρωπαϊκό τουλάχιστον νομικό πολιτισμό. [Καιάφα-Γκμπάντι Μ. (2000) «*Το ποινικό δίκαιο στην καμπή του 2000: Με το βλέμμα προς το μέλλον χωρίς αποτίμηση του παρελθόντος;*», Υπεράσπιση, σελ. 49-50].

αυτό που στη γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «computer sabotage» (δολιοφθορά ηλεκτρονικού υπολογιστή).

4.3.4.5. Κακή χρήση συσκευών (misuse of devises)

Σύμφωνα με το άρθρο 6 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, προκειμένου να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα, η παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιοδήποτε άλλο τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα αδικήματα που θεμελιώνονται στα άρθρα 2-5 της Σύμβασης.

4.3.5. Εγκλήματα σχετιζόμενα με υπολογιστές (Computer related offences)

4.3.5.1. Πλαστογραφία σχετιζόμενη με ηλεκτρονικό υπολογιστή (Computer related forgery[88])

Κατά το άρθρο 7 της Σύμβασης κάθε κράτος - μέλος, που θα αποδεχθεί τη Σύμβαση θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα, η εισαγωγή, η μεταβολή, η διαγραφή ή η απόκρυψη στοιχείων, που έχουν ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων, με στόχο να θεωρηθούν ή να χρησιμοποιηθούν για νόμιμους σκοπούς, σαν να ήταν αυθεντικά, ανεξάρτητα από το εάν τα στοιχεία είναι ευθέως αναγνώσιμα και κατανοητά. Για τη θεμελίωση της ποινικής ευθύνης, ένα μέλος μπορεί να απαιτήσει σκοπό εξαπάτησης ή άλλο παρόμοιο παράνομο σκοπό.

Το προστατευόμενο έννομο αγαθό του άρθρου αυτού είναι το ίδιο με αυτό του άρθρου 216 Π.Κ.[89], δηλαδή η ασφάλεια, η αξιοπιστία, η πίστη και η εγκυρότητα των ηλεκτρονικών

[88] Αναφορικά με τη σχέση Η/Υ και εγκλήματος, ο καθηγητής David Carter μίλησε για τρεις βασικές: τον Η/Υ σαν στόχο (κλοπή ή καταστροφή Η/Υ ή λογισμικού), σαν εργαλείο (κλοπή κωδικών πιστωτικών καρτών,Hacking), σαν μέσο (παραγωγή πλαστών εγγράφων, παιδική πορνογραφία, «πειρατεία» λογισμικού), (http://www.lectlaw. com/files/cri14.htm)

[89] σε συνδ. με άρθρο 13 περ. γ, όπως αυτό προστέθηκε με το άρθρο 2 ν.1805/88

δεδομένων, των οποίων η χρήση μπορεί να έχει έννομες συνέπειες. Η ηλεκτρονική πλαστογραφία ρυθμίστηκε με τη διεύρυνση του άρθρου 13 περ. γ Π.Κ., που έγινε με το άρθρο 2 ν. 1805/88. Σύμφωνα με αυτό ως έγγραφο[90] θεωρείται και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφονται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία[91].

4.3.5.2. Απάτη σχετιζόμενη με ηλεκτρονικό υπολογιστή (Computer related fraud)

Σκοπός του άρθρου αυτού είναι να ποινικοποιήσει κάθε παράνομη παραποίηση που γίνεται κατά τη διαδικασία της επεξεργασίας των δεδομένων, με σκοπό να επιτευχθεί παράνομη μεταφορά ιδιοκτησίας (χρημάτων). Σύμφωνα με το άρθρο 8 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να καθιερώσει ως ποινικό αδίκημα[92], σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως και χωρίς δικαίωμα, την απώλεια περιουσίας με:

α) Οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων υπολογιστών.

β) Οποιαδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών, με σκοπό να επιφέρει χωρίς δικαίωμα και με δόλο οικονομικό όφελος στον εαυτό του ή σε άλλον.

---

[90] η ΑΠ 1992/1984 (Ποιν. Χρον. 1985, σελ. 600) αναφέρει ότι έγγραφο είναι: «*κάθε ανθρώπινη ενέργεια μνημείο, το οποίο περιέχει γραφή ή άλλο σημείο παράστασης εννοιών για γεγονότα που έχουν έννομη σημασία και συνεπώς για την έννοια του εγγράφου σημασία έχει ο προορισμός (ή) η προσφορότητα του να αποδείξει τέτοια γεγονότα*».

[91] βλ. Ειρήνης Βασιλάκη. Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, σειρά ΠΟΙΝΙΚΑ, Νο 40, σελ. 133επ.

[92] βλ. Χρ. Μυλωνόπουλου, Ποινικό Δίκαιο, Ειδικό Μέρος, εκδ. Σάκκουλα, 2000, σελ. 548επ με το άρθρο 5 ν.1805/88.

## 5. Το ευρωπαϊκό δίκαιο

### 5.1. «Απόφαση- πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών»

Η απόφαση αυτή αποτελεί μια από τις σημαντικότερες σε επίπεδο κοινοτικού οργάνου και συμπληρώνει το πλαίσιο ήδη ληφθέντων μέτρων για την καταπολέμηση κάθε μορφής απάτης που διαπράττεται με μέσα πληρωμών πλην των μετρητών. Ορίζει τις απατηλές συμπεριφορές οι οποίες ενδέχεται να συνιστούν ποινική παράβαση που υπόκειται σε κυρώσεις σε όλη την Ένωση, κυρώσεις οι οποίες πρέπει να είναι αποτελεσματικές, ανάλογες και αποτρεπτικές

Η Απόφαση-πλαίσιο[93] του Συμβουλίου της 28ης Μαΐου 2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών ορίζει ως μέσα πληρωμής κάθε ενσώματο μέσο, εκτός από το νόμιμο νόμισμα (τραπεζογραμμάτια και κέρματα) που επιτρέπει, λόγω της ιδιαίτερης φύσης του, μόνο του ή σε συνδυασμό με άλλο μέσο (πληρωμής), στον κάτοχο ή στο χρήστη του να μεταφέρει χρήματα ή νομισματική αξία, όπως π.χ. οι πιστωτικές κάρτες, οι κάρτες των ευρωεπιταγών, λοιπές κάρτες εκδιδόμενες από χρηματοπιστωτικά ιδρύματα, οι ταξιδιωτικές επιταγές, οι ευρωεπιταγές, λοιπές επιταγές και

[93] Η απόφαση-πλαίσιο χρησιμοποιείται για την προσέγγιση των νομοθετικών και κανονιστικών διατάξεων των κρατών μελών. Προτείνεται έπειτα από πρωτοβουλία της Επιτροπής ή κράτους μέλους και πρέπει να εγκριθεί ομόφωνα. Δεσμεύει τα κράτη μέλη ως προς το αποτέλεσμα που πρέπει να επιτευχθεί και αφήνει τις εθνικές αρχές να αποφασίσουν τον τρόπο και τα μέσα με τα οποία θα το πράξουν. Η απόφαση αφορά κάθε άλλο στόχο πλην της προσέγγισης των νομοθετικών και κανονιστικών διατάξεων των κρατών μελών. Έχει δεσμευτικό χαρακτήρα και τα απαραίτητα μέτρα για την εφαρμογή της απόφασης στο επίπεδο της Ευρωπαϊκής Ένωσης εγκρίνονται από το Συμβούλιο με ειδική πλειοψηφία. Η απόφαση-πλαίσιο θεμελιώνεται στη συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ), και ιδίως στο άρθρο 31 στοιχείο (ε) και στο άρθρο 34 παράγραφος 2 στοιχείο (β). Συμφώνως προς το άρθρο 34: "Οι αποφάσεις-πλαίσια δεσμεύουν τα κράτη μέλη ως προς το επιδιωκόμενο αποτέλεσμα αλλά αφήνουν στην αρμοδιότητα των εθνικών αρχών την επιλογή του τύπου και των μέσων". Η νομική πράξη που προσομοιάζει περισσότερο με την απόφαση-πλαίσιο είναι η οδηγία [2]. Και οι δύο πράξεις δεσμεύουν τα κράτη μέλη όσον αφορά το επιδιωκόμενο αποτέλεσμα, αλλά αφήνουν την επιλογή του τύπου και των μεθόδων στην αρμοδιότητα των εθνικών αρχών. Εντούτοις, οι αποφάσεις-πλαίσια δεν παράγουν άμεσο αποτέλεσμα. Πολλές οδηγίες περιέχουν διάταξη που υποχρεώνει τα κράτη μέλη να υποβάλουν εκθέσεις για την υλοποίηση της οδηγίας και παράλληλα υποχρεώνουν την Επιτροπή να καταρτίσει "ενοποιημένη" έκθεση για την εφαρμογή της οδηγίας [3]. Επί τη βάσει των εκθέσεων αυτών, τα θεσμικά όργανα, και ιδίως το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, μπορούν να αξιολογήσουν την έκταση στην οποία τα κράτη μέλη έχουν υλοποιήσει τις διατάξεις της οδηγίας, ούτως ώστε να μπορούν να παρακολουθήσουν την πρόοδο που σημειώνεται σε ένα συγκεκριμένο τομέα κοινοτικού ενδιαφέροντος. Οι οδηγίες εναρμόνισης, ιδίως, αξιολογούνται από την Επιτροπή ως προς την έκταση στην οποία τα κράτη μέλη έχουν εκπληρώσει τις υποχρεώσεις τους. Αυτή η αξιολόγηση μπορεί ενδεχομένως να οδηγήσει σε απόφαση της Επιτροπής να κινήσει διαδικασία παράβασης κατά κράτους μέλους που δεν έχει εκπληρώσει επαρκώς τις υποχρεώσεις του.

συναλλαγματικές, που προστατεύεται από την απομίμηση ή τη δόλια χρήση, παραδείγματος χάριν μέσω σχεδιασμού, κωδικού ή υπογραφής.

Κάθε κράτος μέλος λαμβάνει τα απαραίτητα μέτρα προκειμένου να εξασφαλίσει ότι η κλοπή ή άλλη παράνομη ιδιοποίηση μέσου πληρωμής, η πλαστογράφηση ή παραποίηση μέσου πληρωμής συνιστά ποινικό αδίκημα όταν τελείται εκ προθέσεως, τουλάχιστον όσον αφορά τις πιστωτικές κάρτες, τις κάρτες ευρωεπιταγών, λοιπές κάρτες εκδιδόμενες από χρηματοπιστωτικά ιδρύματα, τις ταξιδιωτικές επιταγές, τις ευρωεπιταγές, λοιπές επιταγές και συναλλαγματικές. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να διασφαλίσει ότι συνιστά ποινικό αδίκημα όταν διαπράττεται εκ προθέσεως η διενέργεια, άμεση ή έμμεση, μεταφοράς χρημάτων ή νομισματικής αξίας, με την οποία επέρχεται σε άλλο πρόσωπο, χωρίς τη συγκατάθεσή του, περιουσιακή ζημιά[94] με πρόθεση την εξασφάλιση παράνομου οικονομικού οφέλους υπέρ του διαπράττοντος το αδίκημα ή τρίτου προσώπου.

Η απόφαση-πλαίσιο 2001/413/ΔΕΥ (εφεξής: απόφαση-πλαίσιο) εξεδόθη στις 28.5.2001 με σκοπό την καταπολέμηση μορφών απάτης και πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών. Της απόφασης-πλαισίου προηγήθηκαν η ανακοίνωση Πλαισίου Δράσης της Επιτροπής και η υποβληθείσα από την Επιτροπή Πρόταση απόφασης-πλαισίου της 14.9.1999 (εφεξής: Πρόταση απόφασης-πλαισίου). Μολονότι η απόφαση-πλαίσιο θέτει στο άρθρο 14 προθεσμία στα κράτη μέλη για την εφαρμογή της ως τις 2.6.2003, η Ελλάδα εξακολουθεί να μην την έχει ενσωματώσει έως σήμερα.

Παρακάτω επιχειρείται μια ανάλυση των κυριότερων σημείων της απόφασης- πλαίσιο, η οποία ουσιαστικά έχει ξεκινήσει από την πρώτη ενότητα με την ανάλυση των άρθρων 1 και 2 σχετικά με τα μέσα πληρωμής πλην των μετρητών τα οποία εδώ θα εξεταστούν εκτενέστερα. Παράλληλα θα παρουσιασθεί και η έκθεση της Επιτροπής που εκπονήθηκε το 2004 κατ' εφαρμογή του άρθρου 14 της απόφασης-πλαισίου του Συμβουλίου της 28ης Μαΐου 2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών, η οποία έκθεση ουσιαστικά αξιολογεί την πρόοδο των κρατών της Ευρωπαϊκής ένωσης σχετικά με τα μέτρα που έλαβαν για την συμμόρφωση με την εν λόγω απόφαση- πλαίσιο.

---

[94] Πρβλ. *Κονταξή* ερμ. ΠΚ σελ 3566. « Η ζημία είναι το οριστικό αποτέλεσμα της επεξεργασίας των στοιχείων μετά τον επηρεασμό των δεδομένων του υπολογιστή. Εάν όμως το αποτέλεσμα αυτό δεν είναι οριστικό αλλά αποτελεί προϋπόθεση για περαιτέρω λήψη αποφάσεως τότε υπάρχει κανονική απάτη με παραπλανηθέν το πρόσωπο που έλαβε υπόψη το άνω αποτέλεσμα

5.1.1. Ποινικά αδικήματα σχετικά με υπολογιστές

Σύμφωνα με το άρθρο 3 της απόφασης-πλαισίου «κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να διασφαλίσει ότι, η ακόλουθη πράξη συνιστά ποινικό αδίκημα όταν διαπράττεται εκ προθέσεως:

Διενέργεια, άμεση ή έμμεση, μεταφοράς χρημάτων ή νομισματικής αξίας, με την οποία επέρχεται σε άλλο πρόσωπο, χωρίς τη συγκατάθεσή του, περιουσιακή απώλεια με πρόθεση την εξασφάλιση παράνομου οικονομικού οφέλους υπέρ του διαπράττοντος το αδίκημα ή τρίτου προσώπου:

- εισάγοντας, αλλοιώνοντας, διαγράφοντας ή εξαλείφοντας χωρίς δικαίωμα δεδομένα υπολογιστή, ιδίως δεδομένα αναγνώρισης της ταυτότητας, ή

- παρεμβαίνοντας χωρίς δικαίωμα στη λειτουργία προγράμματος ή συστήματος υπολογιστή».

Με το άρθρο 3 η Ευρωπαϊκή Ένωση καλύπτει νομοθετικά τον χώρο που επίσης καλύπτει το άρθρο 8 της Σύμβασης του Συμβουλίου της Ευρώπης της 23.11.2001 «για την εγκληματικότητα που σχετίζεται με υπολογιστές».

Το άρθρο 8 της Σύμβασης υποχρεώνει τα μέρη της Συμβάσεως, μεταξύ των οποίων και την Ελλάδα, να τιμωρούν ως εγκλήματα συμπεριφορές πανομοιότυπες με αυτές που προβλέπονται στην απόφαση-πλαίσιο, με μόνη διαφορά ότι η Σύμβαση δεν περιορίζει ρητά το πεδίο εφαρμογής της σε περιουσιακή ζημιά που προκαλείται με τη διενέργεια πράξεων πληρωμής.

5.1.2. Ζημιογόνος ηλεκτρονική πράξη πληρωμής

Η εγκληματική συμπεριφορά εντοπίζεται στη διενέργεια μεταφοράς χρημάτων ή νομισματικής αξίας, δηλαδή στη διενέργεια πράξης πληρωμής, χωρίς τη συγκατάθεση του δικαιούχου του λογαριασμού. Από την πράξη πληρωμής πρέπει να επέρχεται περιουσιακή ζημία στον δικαιούχο. Κάτι τέτοιο δεν συμβαίνει όταν π.χ. η πληρωμή συνίσταται αποκλειστικά στην εκπλήρωση ανειλημμένης από τον δικαιούχο υποχρέωσης, όπως είναι η εξόφληση πληρωτέου λογαριασμού. Η περιουσιακή απώλεια αντανακλάται με τη σειρά της στην υποκειμενική υπόσταση του εκ προθέσεως τελούμενου εγκλήματος, για την πλήρωση

της οποίας απαιτείται περαιτέρω η πρόθεση του δράστη να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος.

Η ιδιομορφία της εν λόγω πράξης πληρωμής έγκειται στη διενέργεια της αμιγώς σε περιβάλλον πληροφορικής. Σε αντίθεση με την δόλια χρήση μέσου πληρωμής[95], που επίσης συνίσταται στη διενέργεια ζημιογόνου πράξης πληρωμής, τα ποινικά αδικήματα του άρθρου 3 δεν φαίνεται να προϋποθέτουν την κατοχή κάποιου μέσου πληρωμής ως ενσώματου μέσου. Σκοπός των σχετικών διατάξεων είναι κυρίως η ποινική θωράκιση των αποϋλοποιημένων τραπεζικών συναλλαγών, όπως αυτών που αφορούν υπηρεσίες διαδικτυακής τραπεζικής (internet banking) και τραπεζικής τηλεξυπηρέτησης μέσω τηλεφώνου. Η απόφαση-πλαίσιο υποχρεώνει τα κράτη μέλη να αναγάγουν τη ζημιογόνο ηλεκτρονική πράξη πληρωμής σε έγκλημα όταν αυτή τελείται με έναν από τους ακόλουθους δυο τρόπους:

- Παρέμβαση χωρίς δικαίωμα στα δεδομένα υπολογιστή

Η παρέμβαση στα δεδομένα υπολογιστή ως τρόπος διενέργειας ζημιογόνου πράξης πληρωμής έγκειται στην χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή. Η Σύμβαση του Συμβουλίου της Ευρώπης «για την εγκληματικότητα που σχετίζεται με υπολογιστές» ορίζει στο άρθρο 1 στοιχ. β' τα «δεδομένα» υπολογιστή ως κάθε γεγονός ή πληροφορία με μορφή κατάλληλη για επεξεργασία από ένα σύστημα υπολογιστή συμπεριλαμβανομένης της επεξεργασίας από ένα πρόγραμμα. Τα δεδομένα αυτά είναι συνήθως δεδομένα αναγνώρισης της ταυτότητας του δικαιούχου[96]

Οι περιπτώσεις παρέμβασης στα δεδομένα υπολογιστή αντιστοιχούν στις συμπεριφορές που περιγράφονται στα στοιχεία στ' έως η' του άρθρου 2 εδ.α' της Πρότασης απόφασης-πλαισίου της Επιτροπής και αφορούν την χρήση αληθών στοιχείων αναγνώρισης της ταυτότητας χωρίς έγκριση του νόμιμου κατόχου, τη χρήση ψευδών/πλαστών στοιχείων αναγνώρισης της ταυτότητας (όχι όμως και τη χρήση ψευδώνυμου από τον νόμιμο κάτοχο) και τις περιπτώσεις που οι πληροφορίες που κυκλοφορούν στο σύστημα επεξεργασίας αλλοιώνονται εκ προθέσεως προκειμένου να καταλογιστεί η εντολή σε λογαριασμό άλλο από εκείνο του νόμιμου δικαιούχου της εντολής. Η περίπτωση του στοιχείου θ' της Πρότασης της Επιτροπής, κατά την οποία τα στοιχεία αναγνώρισης ταυτότητας διαβιβάζονται σε πρόσωπο

[95] Βλ. άρθρου 2 στοιχ. γ'

[96] ονόματα ή ψευδώνυμα και κωδικοί χρήστη

μη εξουσιοδοτημένο να κατέχει τις πληροφορίες αυτές που προτίθεται ή θα μπορούσε να τις χρησιμοποιήσει για να αποκομίσει παράνομο περιουσιακό όφελος, δεν καλύπτεται πλέον αυτοτελώς από την απόφαση-πλαίσιο, παρά μόνο στα πλαίσια της συνέργειας σε απάτη με υπολογιστή[97].

- Παρέμβαση χωρίς δικαίωμα σε πρόγραμμα ή σύστημα υπολογιστή

Την ειδική υπόσταση του εγκλήματος πληροί και όποιος εκ προθέσεως παρεμβαίνει χωρίς δικαίωμα στη λειτουργία προγράμματος ή συστήματος υπολογιστή. Η συμπεριφορά αυτή ενέχει τη μεγαλύτερη δυνατή επικινδυνότητα για τη λειτουργικότητα των συναλλαγών καθώς εκθέτει αόριστο αριθμό νομίμων χρηστών στον κίνδυνο περιουσιακής βλάβης, ο οποίος τελικά πραγματώνεται με τη διενέργεια συγκεκριμένων πράξεων πληρωμής. Ως «σύστημα υπολογιστή» εννοείται εδώ κυρίως το ηλεκτρονικό σύστημα πληρωμών με την έννοια του συνόλου των ηλεκτρονικά, δηλαδή με υπολογιστή, υποστηριζόμενων μέσων, διαδικασιών και κανόνων για τη μεταφορά κεφαλαίων μεταξύ των μετεχόντων στο σύστημα. Η Σύμβαση του Συμβουλίου της Ευρώπης «για την εγκληματικότητα που σχετίζεται με υπολογιστές» ορίζει στο άρθρο 1 στοιχ. α' το «σύστημα υπολογιστών» ως μία εγκατάσταση ή μία ομάδα συνδεδεμένων εγκαταστάσεων, η οποία μόνη της ή όλες μαζί εκτελούν βάσει προγράμματος αυτόματη επεξεργασία δεδομένων. Από τον ορισμό αυτό προκύπτει ότι η παρέμβαση σε σύστημα υπολογιστή γίνεται στην πράξη συνήθως με την παρέμβαση στη λειτουργία προγράμματος.

## 5.2. Έκθεση της Επιτροπής που εκπονήθηκε κατ' εφαρμογή του άρθρου 14 της απόφασης-πλαισίου του Συμβουλίου της 28ης Μαΐου 2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών {SEC(2004) 532} / COM/2004/0346 τελικό

Το άρθρο 14 της απόφασης-πλαισίου της 28ης Μαΐου 2001 υποχρεώνει τα κράτη μέλη να θέσουν σε ισχύ τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την απόφαση-πλαίσιο έως τις 2 Ιουνίου 2003. Έως την ίδια ημερομηνία, τα κράτη μέλη όφειλαν να

[97] Έτσι in concreto η απόφαση *AG Hamm* CR 2006, 70 επ

διαβιβάσουν στη Γενική Γραμματεία του Συμβουλίου και στην Επιτροπή το κείμενο των διατάξεων με τις οποίες μεταφέρθηκαν στην εθνική νομοθεσία οι υποχρεώσεις που επιβάλλει η απόφαση-πλαίσιο. Μέχρι τις 2 Σεπτεμβρίου 2003 το αργότερο, το Συμβούλιο έπρεπε να έχει εξετάσει, βάσει έκθεσης που θα καταρτιζόταν με βάση τις πληροφορίες αυτές και γραπτής έκθεσης της Επιτροπής, κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα ώστε να συμμορφωθούν προς την απόφαση-πλαίσιο.

Έως τις 2 Ιουνίου 2003, εντούτοις, κανένα κράτος μέλος δεν είχε ανακοινώσει στην Επιτροπή τα μέτρα που έλαβε για την υλοποίηση της απόφασης-πλαισίου. Υπ' αυτές τις συνθήκες, η εκπόνηση γραπτής έκθεσης δεν θα είχε νόημα. Έτσι, η Επιτροπή έκρινε σκοπιμότερο να καθυστερήσει την εκπόνηση της έκθεσης, μέχρις ότου λάβει όλες (σχεδόν) τις ανακοινώσεις των κρατών μελών.

Οι εκθέσεις που προβλέπει το άρθρο 14 της απόφασης-πλαισίου αποτελούν την κύρια πηγή πληροφοριών που διαθέτει η Επιτροπή. Η αξία της παρούσας έκθεσης, συνεπώς, εξαρτιόταν σε μεγάλο βαθμό από την ποιότητα και την ακρίβεια των πληροφοριών εθνικής προέλευσης που λαμβάνει η Επιτροπή.

### 5.2.1. Η πορεία προς την υλοποίηση της απόφασης-πλαισίου.

Η έκθεση βασίζεται στις πληροφορίες που διαβιβάστηκαν στην Επιτροπή, οι οποίες συμπληρώθηκαν, εφόσον αυτό είναι απαραίτητο και δυνατό, μέσω περαιτέρω ανταλλαγών με τα εθνικά σημεία επαφής. Οι πληροφορίες που διαβίβασαν τα κράτη μέλη ποικίλλουν σημαντικά, ιδίως όσον αφορά το βαθμό πληρότητάς τους. Ορισμένα κράτη μέλη απέστειλαν πλήρη εθνική νομοθεσία, χωρίς να παράσχουν επεξηγήσεις, αφήνοντας στην Επιτροπή τη φροντίδα να διαπιστώσει αν και κατά πόσον οι εθνικές διατάξεις πληρούν τις απαιτήσεις που τάσσει η απόφαση-πλαίσιο. Άλλα κράτη μέλη διαβίβασαν περισσότερες λεπτομέρειες όσον αφορά το ιστορικό και το χρονοδιάγραμμα έναρξης εφαρμογής. Οι πληροφορίες αυτές, οι οποίες διαβιβάστηκαν στις διάφορες εθνικές γλώσσες κάθε κράτους μέλους, χρειάστηκε να μεταφραστούν στα αγγλικά πριν μπορέσουν να εξεταστούν.

Η Αυστρία, το Βέλγιο, η Ελλάδα, το Λουξεμβούργο απάντησαν στην Επιτροπή χωρίς να αποστείλουν νομοθεσία. Η Αυστρία ενημέρωσε την Επιτροπή ότι η νομοθετική διαδικασία αναμενόταν να ολοκληρωθεί έως τα τέλη του 2003. Το Βέλγιο έκρινε ότι η βελγική νομοθεσία

δεν απαιτεί μέτρα μεταφοράς διότι ευθυγραμμίζεται ήδη με την απόφαση-πλαίσιο, αλλά δεν απέστειλε στην Επιτροπή τα συναφή ισχύοντα νομοθετικά κείμενα. Η Ελλάδα ενημέρωσε την Επιτροπή ότι η ειδική νομοπαρασκευαστική επιτροπή αναμενόταν να παραδώσει το έργο της στα μέσα Ιουλίου 2003. Το Λουξεμβούργο δήλωσε ότι το νομοσχέδιο θα ήταν έτοιμο έως τον Οκτώβριο 2003. Η Δανία και η Πορτογαλία δεν απάντησαν στην Επιτροπή.

Εννέα κράτη μέλη[98] διαβίβασαν στην Επιτροπή το κείμενο των διατάξεων με τις οποίες μεταφέρθηκαν στην εθνική τους νομοθεσία οι υποχρεώσεις που τους επέβαλλε η απόφαση-πλαίσιο. Η Φινλανδία διαβίβασε ένα σημείωμα για τις νομοθετικές τροποποιήσεις οι οποίες τέθηκαν σε ισχύ την 1η Ιουλίου 2003 για τη συμμόρφωση με τις υποχρεώσεις που τάσσει η απόφαση-πλαίσιο, συνοδευόμενο από αποσπάσματα της συναφούς νομοθεσίας. Η Γαλλία απέστειλε στην Επιτροπή σημείωμα στο οποίο περιγράφεται η νέα εθνική νομοθεσία που τέθηκε σε ισχύ ειδικά για τη συμμόρφωση με τα άρθρα 2 έως 12 της απόφασης-πλαισίου, συνοδευόμενο από αποσπάσματα του Ποινικού Κώδικα σχετικά με τα διάφορα αδικήματα. Η νομοθεσία αυτή ισχύει ήδη. Η Γερμανία απέστειλε το πλήρες κείμενο των διατάξεων με τις οποίες μεταφέρθηκαν οι υποχρεώσεις που απορρέουν από την απόφαση-πλαίσιο, συνοδευόμενο από σύντομη ανάλυση των εθνικών διατάξεων. Η Ιταλία απέστειλε σύντομο πίνακα υλοποίησης για τα άρθρα 2, 3, 4 και 7, συνοδευόμενο από αποσπάσματα του Ποινικού Κώδικα. Η Ιρλανδία απέστειλε στην Επιτροπή πίνακα υλοποίησης στον οποίο αναφέρονται εκτενώς συγκεκριμένες διατάξεις της ιρλανδικής νομοθεσίας που αφορούν τα άρθρα 2, 3, 4, 5, 6, 7 και 8 της απόφασης-πλαισίου. Οι Κάτω Χώρες απέστειλαν στην Επιτροπή τις συναφείς τροποποιήσεις του Ποινικού Κώδικα για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών, συνοδευόμενες από πίνακα εθνικών διατάξεων συναφών προς τα άρθρα 2 έως 9 της απόφασης-πλαισίου. Η νομοθεσία αυτή δεν έχει τεθεί ακόμα σε ισχύ. Η Ισπανία απέστειλε πλήρη έκθεση για την εθνική νομοθεσία της σχετικά με όλα τα άρθρα της απόφασης-πλαισίου που χρήζουν μεταφοράς και με τη διαδικασία εκπόνησης νέων μέτρων για τη συμμόρφωση με τα άρθρα 2 έως 7. Η Σουηδία απέστειλε στην Επιτροπή ορισμένα εκτενή κεφάλαια της ποινικής νομοθεσίας της (κεφάλαιο 8 περί κλοπής, ληστείας και λοιπών εγκλημάτων κατά της ιδιοκτησίας, κεφάλαιο 9 περί απάτης και άλλων εγκλημάτων που τελούνται με εξαπάτηση κλπ.) χωρίς περαιτέρω επεξηγήσεις. Το Ηνωμένο Βασίλειο απέστειλε εκτενή νομοθεσία.

[98] Φινλανδία, Γαλλία, Γερμανία, Ιρλανδία, Ιταλία, Κάτω Χώρες, Ισπανία, Σουηδία, Ηνωμένο Βασίλειο

5.2.2. Λοιπά νομοθετήματα

Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος . Στην Ευρωπαϊκή Ένωση ισχύουν :

1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας,

2. Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών

3. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

4. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

5. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.

6. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου [99]εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

---

[99] Το οργανωμένο έγκλημα δεν ορίζεται με ακρίβεια σε κανένα ευρωπαϊκό κείμενο. Βλ. Ελισάβετ Συμεωνίδου – Καστανίδου, Για ένα νέο ορισμό του οργανωμένου εγκλήματος στην Ευρωπαϊκή Ένωση, *Ποινικά Χρονικά* 2006 (Ποιν.Χρον), σελ. 867. Σύμφωνα με την Interpol, ο ορισμός της «ομάδας» οργανωμένου εγκλήματος είναι: «*Μια ομάδα που έχει επιχειρηματική δομή και κύριο αντικείμενό της είναι η πρόσκτηση οικονομικού οφέλους μέσα από παράνομες δραστηριότητες που ευδοκιμούν βασιζόμενες συχνά στο φόβο και τη διαφθορά*». Ο ορισμός αυτός, όπως είναι ευνόητο, είναι πολύ γενικός και άλλοτε υπερκαλύπτει, άλλοτε υπολείπεται στην περιγραφή των πράξεων του οργανωμένου εγκλήματος. Η Ευρωπαϊκή Ένωση έχει υιοθετήσει ένα άλλο τρόπο περιγραφής της έννοιας του οργανωμένου εγκλήματος. Χρησιμοποιεί για αυτό το σκοπό έντεκα κριτήρια με βάση τα οποία γίνεται η διάκριση της ύπαρξης ή όχι οργανωμένου εγκλήματος σε μια οποιαδήποτε εγκληματική ενέργεια.

7. Το Σχέδιο Δράσης με αριθμό 97/C 251/01για την καταπολέμηση του οργανωμένου εγκλήματος.

## 6. Το ελληνικό δίκαιο

### 6.1. Γενικά

Στην ελληνική έννομη τάξη, νομοθεσία ειδική για θέματα Διαδικτύου που να ρυθμίζει τη συμπεριφορά των χρηστών του δεν υπάρχει. Ο όρος 'ηλεκτρονικό έγκλημα' δεν αναφέρεται πουθενά στο ελληνικό δίκαιο. Οι παραβάσεις που διαπιστώνονται για οικονομικά ή μη, αδικήματα που διαπράττονται μέσω Διαδικτύου τιμωρούνται σύμφωνα με τη νομοθεσία της κλασικής μορφής τέλεσης των αδικημάτων αυτών. Ισχύουν νόμοι για εγκλήματα που διαπράττονται με Η/Υ (1805/1988), για την προστασία προσωπικών δεδομένων από τη χρήση των τηλεπικοινωνιών (2867/2000, ο οποίος αντικατέστησε τον 2246/1994), την προστασία προσωπικών δεδομένων κατά τη χρήση του Διαδικτύου (2774/1999, σε συνδυασμό με 2472/1997), την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας (2225/1994, σε συνδυασμό με 3115/2003) κ.λ.π.

Ειδικά ο Ν. 1805/1988[100], τροποποίησε - συμπλήρωσε τις σχετικές διατάξεις του Π.Κ, που αφορούν τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. Πιο συγκεκριμένα προστέθηκαν τέσσερα εμβόλιμα άρθρα: εδαφ.β΄ στο άρθρο 13 περ.γ΄ (που περιγράφεται η έννοια του εγγράφου), 370β, 370γ και 386α. Σημεία αναφοράς του αξιόποινου αποτελούν οι διατάξεις της πλαστογραφίας εγγράφου (άρθρο 216 ΠΚ) και της απάτης με υπολογιστή (άρθρο 386Α ΠΚ)[101], ενώ ερευνητέα είναι κατά περίπτωση η πλήρωση της ειδικής υπόστασης και άλλων εγκλημάτων.

---

[100] Αναλυτικά για το Ν. 1805/1988 βλ. *Χ. Μυλωνόπουλος*, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991

[101] Το εν λόγω άρθρο προστέθηκε στον Ελληνικό Ποινικό Κώδικα με τον Ν.1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του Ποινικού Κώδικα (άρθρα: 13γ, 370Β, 370Γ, 386Α Π.Κ) οι οποίες αφορούν τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes). Για την εποχή του θεωρήθηκε αρκετά πρωτοποριακό. Διαμορφώθηκε ακολουθώντας ως πρότυπο την αντίστοιχη γερμανική διάταξη του άρθρου 263Α του Γερμανικού Ποινικού Κώδικα (263a StGB), η οποία με τη σειρά της είχε εισαχθεί στην Γερμανία μόλις δύο χρόνια νωρίτερα, το έτος 1986.

## 6.2. Η απουσία ενσωμάτωσης του κοινοτικού δικαίου

Αν και η απόφαση-πλαίσιο θέτει στην παράγραφο 1 του άρθρου 14 ως προθεσμία για την εφαρμογή της τις 2.6.2003, ο Έλληνας νομοθέτης σε αντίθεση σχεδόν με όλους τους άλλους νομοθέτες κρατών μελών της ΕΕ εξακολουθεί να μην την έχει ενσωματώσει στο ελληνικό ποινικό δίκαιο. Η σύσταση ειδικής νομοπαρασκευαστικής επιτροπής για την ενσωμάτωση της απόφασης-πλαισίου στην ελληνική νομοθεσία επιτρέπει ωστόσο την πρόβλεψη της επικείμενης ενσωμάτωσης. Μέχρι τότε το ελληνικό ποινικό δίκαιο καλείται να αντιμετωπίσει τις εγκληματικές συμπεριφορές που περιγράφονται στα άρθρα 2, 3 και 4 της απόφασης-πλαισίου με το υπάρχον νομοτυπικό οπλοστάσιο.

### 6.2.1. Κλοπή ή υπεξαίρεση μέσου πληρωμής

Οι εγκληματικές συμπεριφορές τού άρθρου 2στοιχ. α' της απόφασης πλαισίου τιμωρούνται κατά το ισχύον ελληνικό ποινικό δίκαιο με βάση τις διατάξεις περί κλοπής[102] ληστείας[103] και υπεξαίρεσης[104], ως εγκλήματα δηλαδή κατά της ιδιοκτησίας. Προκειμένου περί κάρτας πληρωμής ή αξιογραφικού νομίσματος υποστηρίζεται ωστόσο βάσιμα η ειδικότερη εφαρμογή της προνομιούχου περίπτωσης κλοπής ή υπεξαίρεσης[105], η οποία προβλέπει μειωμένη ποινή για πράγματα «ευτελούς αξίας».

### 6.2.2. Πλαστογραφία μέσου πληρωμής

Η πλαστογραφία, ως οικονομικό ηλεκτρονικό έγκλημα, εμφανίζεται κατεξοχήν στο πλαίσιο της εγκληματικής δραστηριότητας που κατατείνει τελικά στη διάπραξη της απάτης με υπολογιστή με την μορφή του phishing ή του pharming. Στην περίπτωση του phishing, που περιγράψαμε πιο πάνω, ο δράστης επικοινωνεί με το θύμα του αποστέλλοντας μια

[102] Βλ. άρθρο 372 ΠΚ

[103] Βλ. άρθρο 380 ΠΚ

[104] Βλ. άρθρο 375 ΠΚ

[105] Βλ. άρθρο 377 ΠΚ

ηλεκτρονική επιστολή, δηλ. ένα πλαστό έγγραφο, το οποίο παραπλανά ως προς την ταυτότητα του εκδότη του. Προκειμένου δηλ. να παραπλανήσει το θύμα του και να αποσπάσει τους κωδικούς του λογαριασμού (PIN και άλλα στοιχεία) καταρτίζει ένα πλαστό έγγραφο, το οποίο φέρεται να προέρχεται από την τράπεζα ή από άλλο πιστωτικό οργανισμό ή εταιρεία ασφάλειας συστημάτων κ.λπ.. Η ηλεκτρονική επιστολή εντάσσεται στην έννοια του εγγράφου[106] κατ' άρθρο 13 γ΄ Π.Κ. και επιτελεί και τις τρεις λειτουργίες του (αποδεικτική, διαιωνιστική, εγγυητική)[107]. Μάλιστα, όπως έχει επισημανθεί, τα στοιχεία που δηλώνουν την ταυτότητα του εκδότη (ηλεκτρονική διεύθυνση και λοιπά στοιχεία επικοινωνίας) εμφανίζουν, σε σχέση με άλλες μορφές επικοινωνίας (π.χ. φαξ), υψηλότερο βαθμό ασφάλειας[108].

Η «πλαστογράφηση ή παραποίηση μέσου πληρωμής προκειμένου να χρησιμοποιηθεί δολίως»[109] τιμωρείται κατά το ισχύον ελληνικό ποινικό δίκαιο ως πλαστογραφία εγγράφου[110]. Αυτό είναι προφανές για τα αξιγραφικά «μέσα πληρωμής πλην των μετρητών», δηλαδή τις ταξιδιωτικές επιταγές, τις ευρωεπιταγές και τις λοιπές επιταγές και συναλλαγματικές, τα οποία ως γραπτά πρόσφορα να αποδείξουν γεγονός που έχει έννομη σημασία εμπίπτουν στην παραδοσιακή έννοια του εγγράφου κατά το άρθρο 13 παρ. γ' εδ. α' ΠΚ. Στο εδάφιο β' του ίδιου άρθρου όμως η έννοια του εγγράφου διευρύνεται σημαντικά για να συμπεριλάβει και τις ηλεκτρομαγνητικές και μαγνητικές εγγραφές σε υλικούς φορείς δεδομένων. Με έγγραφο εξομοιώνονται έτσι όλες οι κάρτες πληρωμής που εμπίπτουν στο πεδίο εφαρμογής της απόφασης-πλαισίου (πχ. πιστωτική ή χρεωστική κάρτα με μαγνητοταινία, προπληρωμένη κάρτα πολλαπλών χρήσεων με μικροεπεξεργαστή, δίσκος ηλεκτρονικού υπολογιστή με αποθηκευμένες μονάδες ηλεκτρονικού χρήματος).

Η πλαστογραφία μέσων πληρωμής δεν μπορεί αντιθέτως να τιμωρηθεί ως παραχάραξη[111], καθώς η παραχάραξη προϋποθέτει νόμισμα με τη στενή έννοια του όρου ή

---

[106] Για τις λειτουργίες του εγγράφου βλ. *Μυλωνόπουλου* Ποινικό Δίκαιο Ειδικό Μέρος εγκλήματα σχετικά με τα υπομνήματα σελ 8 επ

[107] Δ.Κιούπη ό.π., σελ.157, Α. Κωνσταντινίδη, Η έννοια και λειτουργία του εγγράφου στο ουσιαστικό και δικονομικό ποινικό δίκαιο 2000, σελ.117 επ., Μυλωνόπουλου ό.π.,31. Έτσι και ειδικά για την περίπτωση του phishing M. Gercke, ό.π., σελ. 611.

[108] Βλ. .Κιούπη ό.π., σελ. 158

[109] Βλ. άρθρο 2 στοιχ. β' της απόφασης-πλαισίου 2001/413 ΔΕΥ

[110] Βλ. άρθρο 216 ΠΚ

[111] Βλ. άρθρο 207 ΠΚ

κάποιο από τα οριζόμενα περιοριστικά στο άρθρο 214 ΠΚ αξιογραφικά νομίσματα. Ειδικότερα η εφαρμογή του άρθρου 214 ΠΚ65 επί επιταγών και συναλλαγματικών θα συνιστούσε, παρά την αξιολογική ομοιότητα των συμπεριφορών, ανεπίτρεπτη αναλογική εφαρμογή ποινικού νόμου προς θεμελίωση του αξιόποινου.

6.2.3. Χρήση κλεμμένου, παράνομα ιδιοποιημένου ή πλαστού μέσου πληρωμής

Η απατηλή χρήση πλαστού μέσου πληρωμής, δηλαδή η χρήση του πλαστού με σκοπό προσπορισμού παράνομου περιουσιακού οφέλους", τιμωρείται κατά το ισχύον δίκαιο ως χρήση πλαστού εγγράφου[112]. Κατ' αντιστοιχία με τα ισχύοντα στα συνήθη υπομνήματα, η χρήση του πλαστού μέσου πληρωμής θα στοιχειοθετείται αντικειμενικά όταν ο δράστης καταστήσει τούτο προσιτό στον μέλλοντα να παραπλανηθεί αντισυμβαλλόμενό του. Στην πράξη θα πρέπει το μέσο πληρωμής να μετακινηθεί από τη σφαίρα κυριαρχίας του δράστη στη σφαίρα κυριαρχίας του συναλλασσόμενου με τον δράστη. Αρκεί η δυνατότητα παραπλάνησης του τρίτου, δηλαδή η δυνατότητα αποδοχής του πλαστού μέσου πληρωμής από τον συναλλασσόμενο, χωρίς να απαιτείται πράγματι αποδοχή της προσφοράς ή εντολής πληρωμής και ολοκλήρωση της συναλλαγής. Για το αξιόποινο[113] κατ' άρθρο 216 παρ. 2 ΠΚ δεν απαιτείται να χρησιμοποιηθεί το πλαστό μέσο πληρωμής μέσα στο πλαίσιο διενέργειας στενά εννοουμένης πράξης πληρωμής.

Ο δράστης, ο οποίος μπορεί να είναι και τρίτο πρόσωπο πέραν του πλαστογράφου, πρέπει να τελεί εν γνώσει της πλαστότητας του μέσου πληρωμής. Ο ενδεχόμενος δόλος δεν αρκεί[114]. Επειδή ο δράστης πρέπει να κάνει χρήση του πλαστού εγγράφου «με σκοπό να παραπλανήσει με τη χρήση του άλλον», μόνο η χρήση τέτοιων μέσων πληρωμής, τα οποία απευθύνονται σε φυσικά πρόσωπα πληροί την υποκειμενική υπόσταση του άρθρου 216 παρ. 2 ΠΚ. Τέτοια μέσα πληρωμής είναι κατεξοχήν οι επιταγές και οι συναλλαγματικές αλλά και οι κάρτες πληρωμής, που δεν τίς επεξεργάζονται απευθείας μηχανήματα/υπολογιστές σε αμιγώς

[112] Βλ. άρθρο 216 παρ. 2 ΠΚ

[113] Αρκεί και η χρήση του πλαστού μέσου πληρωμής ως εγγύησης , π.χ. η χρήση της τραπεζικής επιταγής, ως εγγύησης για την καλή εκπλήρωση σύμβασης ή της πιστωτικής κάρτας , ως εγγύησης για την ενοικίαση αυτοκινήτου

[114] Βλ. άρθρο 2 παρ. Ζ εδ. α' ΠΚ

αυτοματοποιημένες διαδικασίες αλλά «περνάνε» και από φυσικά πρόσωπα (πχ. ταμίας που παίρνει πιστωτική κάρτα και ελέγχει τη γνησιότητά της και τη νομιμοποίηση του κατόχου πριν την περάσει για έγκριση και χρέωση από το τερματικό μηχάνημα της τράπεζας).

Η αποτυχία της παραπλάνησης, όταν ο ταμίας διαπιστώνει την πλαστότητα της κάρτας και αρνείται τη συναλλαγή, αποκτά σημασία μόνο στο πλαίσιο συρροής της χρήσης πλαστού με την απάτη[115]. Η μη αποδοχή του πλαστού εγγράφου/μέσου πληρωμής αποτρέπει την περιουσιακή διάθεση και την περιουσιακή βλάβη του συναλασσόμενου ή τρίτου προσώπου (ανάλογα με τον καταμερισμό της αστικής ευθύνης με βάση τον εκάστοτε συμβατικό τύπο και τους σχετικούς Γενικούς Όρους των Συναλλαγών), οπότε θεμελιώνεται μόνο απόπειρα απάτης.

Στις άλλες περιπτώσεις μέσων πληρωμής (πχ. κάρτα ανάληψης μετρητών από ΑΤΜ), όπου για τη διενέργεια της πληρωμής δεν έρχεται σε ουσιαστική επαφή με το μέσο πληρωμής άνθρωπος, η χρήση του μέσου πληρωμής τιμωρείται κατά το ισχύον δίκαιο ως απάτη με υπολογιστή[116].

### 6.2.4. Συνοδευτικές πράξεις

Η αποδοχή, κτήση, κατοχή, μεταφορά, πώληση ή μεταβίβαση κλεμμένου ή άλλως παρανόμως ιδιοποιημένου (πχ. υπεξαιρεθέντος) ή πλαστού μέσου πληρωμής (άρθρο 2 στοιχ. γ' της απόφασης-πλαισίου), στο βαθμό που τα μέσα πληρωμής της απόφασης-πλαισίου δεν απολαμβάνουν (ακόμα) την ποινική προστασία του άρθρου 207 ΠΚ, εκτιμώνται ποινικά μόνο στο πλαίσιο της αποδοχής και διάθεσης προϊόντων εγκλήματος[117]. Δεδομένου όμως ότι το άδικο της αποδοχής εντοπίζεται στη συντήρηση (διαιώνιση) της περιουσιακής προσβολής που προήλθε από προηγούμενη αξιόποινη πράξη, γίνεται δεκτό ότι το υλικό αντικείμενο («πράγμα») της αποδοχής πρέπει να προέρχεται από έγκλημα που προσβάλλει περιουσιακά δικαιώματα εν γένει, δηλαδή έγκλημα κατά της ιδιοκτησίας ή της περιουσίας αλλά και κάθε άλλο έγκλημα που συμπροσβάλλει και την περιουσία, γενικά ή και κατά περίπτωση. Με βάση την παραδοχή αυτή γίνεται δεκτό από την κρατούσα άποψη, που δεν θεωρεί ότι τα εγκλήματα

[115] Βλ. άρθρο 386 ΠΚ

[116] Βλ. άρθρο 386Α ΠΚ

[117] Βλ. άρθρο 394 ΠΚ

περί το νόμισμα προσβάλλουν και την περιουσία, ότι δεν μπορεί να στοιχειοθετήσει αποδοχή πράγμα προερχόμενο από έγκλημα περί το νόμισμα. Μπορεί επομένως να στοιχειοθετήσει αποδοχή κατά το ισχύον δίκαιο το μέσο πληρωμής που προέρχεται από κλοπή, άλλη παράνομη ιδιοποίηση ή κατά περίπτωση πλαστογραφία.

### 6.2.5. Απάτη με υπολογιστή

Επειδή μόνον τα φυσικά πρόσωπα πλανώνται και μόνον η επενέργεια στο νοητικό ανθρώπου συνιστά πράξη εξαπάτησης κατά το άρθρο 386 ΠΚ (απάτη), η «παραπλάνηση» μηχανήματος/ηλεκτρονικού υπολογιστή δεν συνιστά απάτη αλλά το ιδιώνυμο έγκλημα της απάτης με υπολογιστή (άρθρο 386$^{A}$ ΠΚ)[118]. Κοινή απάτη στοιχειοθετείται αντιθέτως, έστω και αν, έχει γινει επέμβαση στο πρόγραμμα ή τη λειτουργία υπολογιστή, όταν μέσω της επέμβασης στη μηχανή πλανάται για να προβεί στη συνέχεια σε ζημιογόνο περιουσιακή διάθεση φυσικό πρόσωπο, δηλαδή η μηχανή χρησιμοποιείται απλώς ως όργανο μεταφοράς της ψευδούς παράστασης (π.χ. η ηλεκτρονική [on-line] εντολή πληρωμής δεν εκτελείται αυτόματα, αλλά εμφανίζεται στην οθόνη υπολογιστή υπαλλήλου της τράπεζας που την ελέγχει και την εκτελεί. Το έγκλημα του άρθρου 386Α ΠΚ επαρκεί νομοτυπικά για την τιμωρία των αδικημάτων που σχετίζονται με υπολογιστές κατ' άρθρο 3 της απόφασης-πλαισίου.

### 6.2.6. Προπαρασκευαστικές πράξεις

Οι απλές προπαρασκευαστικές πράξεις μένουν στο ελληνικό ποινικό δίκαιο κατ' αρχήν ατιμώρητες. Οι ανεπιτυχείς προσπάθειες προσβολής των εννόμων αγαθών τιμωρούνται με τις

---

[118] βλ. ΑΠ 1277/1998 Ποιν. 1999.113 η οποία δέχθηκε ότι η απάτη με ηλεκτρονικό υπολογιστή (άρθρο 386α Π.Κ.) είναι «διαφορετικό έγκλημα» από την απάτη (άρθρο 386 Π.Κ.). Στην εν λόγω απόφαση, ο Άρειος Πάγος διαχώρισε το άρθρο 386 Π.Κ. από το άρθρο 386 *Α* Π.Κ. με τη βασική σκέψη ότι το άρθρο 386 Π.Κ. περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση φυσικού προσώπου, ενώ στο άρθρο 386 *Α* Π.Κ. η ξένη περιουσία βλάπτεται, ασχέτως παραπλανήσεως, με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων υπολογιστή. Βλ. επίσης, ΑΠ 1152/1999 Ποιν. 2000.141, όπου τονίζεται ότι το έγκλημα του άρθρου 386α Π.Κ. τελείται αποκλειστικά και μόνο με το επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του συστήματος και την επεξεργασία των δεδομένων, σε οποιαδήποτε φάση λειτουργίας του υπολογιστή και όχι με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κλπ. Βλ. επίσης, Κουράκης, Ν. & Πατεράκης Ν. (2001) «*Το έγκλημα της απάτης*», Νομική Βιβλιοθήκη, σελ. 209

διατάξεις περί απόπειρας[119], που προϋποθέτει αρχή εκτέλεσης του εγκλήματος, και οι βοηθητικές πράξεις σ' αυτήν της κύριας εγκληματικής πράξης με τις γενικές διατάξεις περί συμμετοχής (άρθρο 46 επ. ΠΚ). Κατ' εξαίρεση τιμωρούνται επομένως οι προπαρασκευαστικές πράξεις, όταν το ορίζει ειδικά νόμος. Η αυτοτελής εγκληματοποίηση προπαρασκευαστικών πράξεων είναι χαρακτηριστική μορφή "προσώθησης του αξιόποινου" (Vorverlagerung der Strafbarkeit).Η συχνή αυτή στο χώρο του οικονομικού ποινικού δικαίου νομοθετική επιλογή εξυπηρετεί σε επίπεδο αντεγκληματικής πολιτικής την ποινικοποίηση προγενέστερων της βλάβης του εννόμου αγαθού συμπεριφορών και σε ποινικοδικονομικό επίπεδο την παράκαμψη αποδεικτικών δυσχερειών.

Η απόφαση-πλαίσιο υποχρεώνει σε εγκληματοποίηση της προπαρασκευής της πλαστογραφίας μέσων πληρωμής και της απάτης με υπολογιστή. Οι προπαρασκευαστικές πράξεις των σχετικών εγκλημάτων, σε αντίθεση με τις προπαρασκευαστικές πράξεις της παραχάραξης νομίσματος[120], δεν τιμωρούνται κατά το ελληνικό ποινικό δίκαιο, οπότε και προκύπτει ανάγκη εναρμόνισης.

### 6.2.7. Ευθύνη νομικών προσώπων

Το ελληνικό ποινικό δίκαιο κατ' απαρέγκλιτη εφαρμογή της αρχής "societas delinquere non potest" αρνείται να αναγνωρίσει την ποινική ευθύνη των νομικών προσώπων. Η απαίτηση «πράξης», ενοχής και ικανότητας αντίληψης του τιμωρητέου χαρακτήρα της ποινής ως θεμελιώδεις εκφάνσεις του ποινικού δόγματος, που κατοχυρώνονται και συνταγματικά (πρβλ. Άρθρα 2, 5, 7, 25 Σ), περιορίζουν την ποινική ευθύνη αυστηρά στα φυσικά πρόσωπα.

Αξιόλογες προσπάθειες γεφύρωσης των ποινικοδογματικών ενστάσεων και του αντεγκληματικού ελλείμματος συνιστούν η πρόταση του *Κουράκη* για τη θέσπιση «οικονομικών ποινών» σε βάρος των νομικών προσώπων κατά το πρότυπο του γερμανικού νόμου περί παραβάσεων τάξεως (α. 30 Ordnungswidrigkeitengestz), καθώς και η ακολουθούσα το ιταλικό παράδειγμα πρόταση του *Σπινέλλη* για την εισαγωγή μίας οιονεί

[119] Βλ. άρθρο 42 επ. ΠΚ

[120] Βλ. άρθρο 211 ΠΚ

ποινικής ευθύνης νομικών προσώπων με την επιβολή κυρώσεων-«μέτρων»[121] ως ενός είδους μέτρων ασφαλείας σε βάρος των επικίνδυνων αλλά ανίκανων για καταλογισμό νομικών προσώπων.

Επομένως, στο πλαίσιο το ισχύοντος ελληνικού δικαίου οι προβλεπόμενες στα άρθρα 7 και 8 της απόφασης-πλαισίου υποχρεώσεις των κρατών μελών μόνο με την καθιέρωση αστικής και (κυρίως) διοικητικής φύσης κυρώσεων μπορούν να εκπληρωθούν. Το ισχύον δίκαιο δεν προβλέπει πάντως τέτοιες κυρώσεις για τις αναφερόμενες στα άρθρα 2 στοιχ. β', γ', δ, 3 και 4 της απόφασης-πλαισίου πράξεις. Αξίζει πάντως να σημειωθεί η εισαγωγή με τον ν. 2948/2001 αντίστοιχης εμβέλειας διοικητικών κυρώσεων για τα σχετικά με το νόμισμα εγκλήματα.

### 6.2.8. Εποπτικές αρχές για την προστασία του διαδικτύου στην Ελλάδα

Οι αρχές που εποπτεύουν σε ζητήματα ασφαλείας του Διαδικτύου και των επικοινωνιών γενικότερα στην Ελλάδα είναι :

- ✓ η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία έχει ως αποστολή την εποπτεία τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο
- ✓ η Αρχή Διασφάλισης του Απορρήτου των επικοινωνιών (Α.Δ.Α.Ε.), σκοπός της οποίας είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο και
- ✓ η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), η οποία χορηγεί άδειες σε Παρόχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's), ενώ ρυθμίζει και ελέγχει τον τομέα των τηλεπικοινωνιών, εποπτεύοντας παράλληλα την τηλεπικοινωνιακή αγορά.

[121] βλ. άρθρο 96 παρ. 1

### 6.2.9. Ποινικοδογματικός προβληματισμός

Από την προηγηθείσα ανάλυση και ερμηνεία του ευρωπαϊκού και του ελληνικού δικαίου προέκυψε η ανάγκη διευκρίνησης του εννόμου αγαθού[122] που προστατεύεται από τις διατάξεις που αφορούν τα μέσα πληρωμής πλην των μετρητών. Ο σχετικός ποινικοδογματικός προβληματισμός επικεντρώνεται στην πλαστογραφία μέσων πληρωμής. Κοινό χαρακτηριστικό τόσο του νομίσματος (με την στενή ή την αξιογραφική έννοια) όσο και των άλλων μέσων πληρωμής πλην των μετρητών αποτελεί ο ενσώματος χαρακτήρας τους. Τα μέσα πληρωμής ως πράγματα αποτελούν το υλικό αντικείμενο της πράξης πλαστοποίησης.

Κοινό χαρακτηριστικό των «μέσων πληρωμής πλην των μετρητών» με τη σειρά τους, είναι η ιδιαίτερη χρηστικότητα τους, η οποία πηγάζει ανάλογα με τη συμβατική τυποποίηση του εκάστοτε μέσου, σε μικρότερο ή μεγαλύτερο βαθμό από την εγγυητική και αποδεικτική τους λειτουργία. Η εγγυητική λειτουργία των μέσων πληρωμής έγκειται στο γεγονός ότι ο εκδότης τους αναλαμβάνει κάποια μορφή ευθύνης, όχι τόσο για το ενσωματωμένο διανόημα, όσο για την πληρωμή. Η ευθύνη αυτή διαμορφώνεται στο εκάστοτε μέσο κατά το αστικό και εμπορικό δίκαιο.

Συχνό κοινό χαρακτηριστικό των «μέσων πληρωμής πλην των μετρητών» είναι ότι αφορούν τριμερείς (τριπρόσωπες) σχέσεις. Προκειμένου περί πιστωτικής κάρτας, η τράπεζα δεσμεύεται από τη σύμβαση παροχής υπηρεσιών κάρτας έναντι του επιχειρηματία σε εξόφληση του, ανεξάρτητα από την φερεγγυότητα του κατόχου/καταναλωτή. Όσον αφορά τα αξιογραφικά μέσα πληρωμής, παρατηρούμε ότι τόσο η επιταγή όσο και η συναλλαγματική είναι αξιόγραφα με τριμερή/εκταξιακό χαρακτήρα, ενσωματώνουν δηλαδή εντολή του εκτάσσοντος προς τον εκτασσόμενο και αντίστοιχη ευθύνη του τελευταίου για πληρωμή του κομιστή τους. Προκειμένου για τις κάρτες ανάληψης απουσιάζει μεν η εν είδη τριμερούς σχέσης εγγυητική τους λειτουργία, ωστόσο αυτές εμφανίζουν κυρίως αποδεικτική χρηστικότητα ως μέσα νομιμοποίησης του κομιστή και του κατόχου του λογαριασμού.

Σκοπός της ποινικής προστασίας των παραπάνω μέσων πληρωμής, όπως και του νομίσματος, είναι επομένως η προστασία της λειτουργικότητας των χρηματικών συναλλαγών (Funktionnsfahigkeit des Zahlungsverkehrs) με την ευρεία έννοια. Η προβαλλόμενη ως

---

[122] Βλ. *Νούσκαλη*, Απάτη με Η/Υ το παρελθόν και το μέλλον του άρθρου 386Α Π.Κ ιδίως υπό το πρίσμα των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, Ποιν Δικ 2/2003, σελ 179

αυτοτελές έννομο αγαθό «εμπιστοσύνη» των συναλλασσομένων στη λειτουργικότητα των χρηματικών συναλλαγών θα πρέπει αντιθέτως να γίνεται αντιληπτή ως αποτέλεσμα και όχι ως σκοπος (ratio) της ποινικής προστασίας.

Παράλληλα με το υπερατομικό έννομο αγαθό της λειτουργικότητας των χρηματικών με ευρεία έννοια συναλλαγών, τα εγκλήματα τα σχετικά με τα πλαστά (αλλά και τα κλεμμένα ή άλλως παρανόμως ιδιοποιημένα) μέσα πληρωμής προσβάλλουν σε βαθμό αφηρημένης διακινδύνευσης και την περιουσία του εκάστοτε μέλλοντος να συναλλαγεί με αυτά. Η αφηρημένη αυτή διακινδύνευση εντείνεται όσο πλησιάζουμε από την προπαρασκευή στην τέλεση της κύριας εγκληματικής πράξης, και από εκεί προς τη συνοδευτική της πράξη και τέλος στην απατηλή χρήση του μέσου πληρωμής. Η προστασία της ατομικής περιουσίας αποτυπώνεται και στη νομοτυπική μορφή των εγκλημάτων: η πλαστογραφία ή η συνοδευτική της πράξη πρέπει να τελούνται «προκειμένου (το πλαστό μέσο πληρωμής) να χρησιμοποιηθεί δολίως», δηλ. με σκοπό την τέλεση απάτης. Η προσβολή του υπερατομικού έννομου αγαθού συγκεντρώνει ωστόσο το κυρίως βάρος του αδίκου, ώστε από μόνη της η αφηρημένη διακινδύνευση της περιουσίας να μην επαρκεί για τη θεμελίωση του αξιόποινου.

6.2.10. Προοπτικές de lege ferenda και de lege europeana lata

Βασική αρχή για την κρίση περί της επάρκειας της συμμόρφωσης του ελληνικού ποινικού δικαίου με τις επιταγές εγκληματοποίησης της απόφασης-πλαισίου είναι ένας «κανονιστικός μινιμαλισμός» που τουλάχιστον οφείλει να διέπει το ευρωπαϊκό δίκαιο, με την έννοια ότι αυτό θεσπίζει μόνο ελάχιστα επίπεδα (ποινικής) προστασίας, σε σχέση με τα οποία ο εθνικός νομοθέτης μπορεί να «πλειοδοτεί» σε ρυθμιστικό εύρος («πλάτος») και κυρωτική ένταση («βάθος»).

Η τιμώρηση της κλοπής και της υπεξαίρεσης μέσων πληρωμής κατ' άρθρο 377 ΠΚ λόγω της ευτελούς αξίας των υλικών αντικειμένων δεν είναι δικαιοπολιτικά ικανοποιητική. De lege ferenda καλείται επομένως ο Έλληνας νομοθέτης είτε να εισαγάγει μια νέα περίπτωση διακεκριμένης κλοπής[123] προκειμένου περί μέσων πληρωμής είτε, κατά προτίμηση, να προσθέσει την κλοπή και υπεξαίρεση μέσων πληρωμής ως νέο αυτοτελές έγκλημα στο Κεφάλαιο Θ' του ΠΚ. Η τελευταία λύση προκρίνεται ενόψει του γεγονότος οτι τα μέσα πληρωμής, ιδίως αυτά που λειτουργούν μόνο νομιμοποιητικά χωρίς να

[123] Βλ. άρθρο 374 ΠΚ

ενσωματώνουν αξία, εκπληρώνουν μια συναλλακτική λειτουργία η προσβολή της οποίας δεν μπορεί να συν(απ)αξιολογηθεί επαρκώς στα πλαίσια των εγκλημάτων κατά της ιδιοκτησίας.

Αντεγκληματικά ανεπαρκής είναι όμως και η τιμώρηση κατά το ισχύον δίκαιο της πλαστογραφίας μέσων πληρωμής ως απλής πλαστογραφίας εγγράφων[124]. Τα ιδιαίτερα ποιοτικά χαρακτηριστικά των «μέσων πληρωμής πλην των μετρητών» σε σχέση με τα κοινά υπομνήματα αξιώνουν αφενός την αυτοτελή προστασία των πρώτων και αφετέρου αυστηρότερο πλαίσιο ποινή κατ' αναλογία με τις κακουργηματικού χαρακτήρα κυρώσεις των άρθρων 207 και 208 ΠΚ. Για την επιβεβλημένη ένταξη των «μέσων πληρωμής πλην των μετρητών» στην ποινική προστασία του Θ' Κεφαλαίου του ΠΚ προσφέρεται η ενσωμάτωσή τους στο άρθρο 214 ΠΚ. Ο εκσυγχρονισμός της έννοιας του «αξιογραφικού» νομίσματος είναι προ πολλού υπερήμερος και η προσθήκη των τραπεζικών καρτών πληρωμής πλέον και de lege lata europeana επιβεβλημένη. Συνεπής με την διεύρυνση του κύκλου των υλικών αντικειμένων των άρθρων 207 επ. ΠΚ θα ήταν και η αλλαγή του τίτλου του Θ' Κεφαλαίου από «εγκλήματα σχετικά με το νόμισμα» σε «εγκλήματα σχετικά με το νόμισμα και τα λοιπά μέσα πληρωμής» ή γενικά σε «εγκλήματα σχετικά με τα μέσα πληρωμής».

Όσον αφορά την χρήση πλαστών «μέσων πληρωμής πλην των μετρητών», η εξομοίωσή τους με το νόμισμα και η τιμώρηση[125] θα οδηγήσει όχι μόνο σε αυστηρότερες ποινές σε σχέση με αυτές του σήμερα εφαρμοζόμενου άρθρου 216 ΠΚ, αλλά και σε διαφορετικούς όρους του αξιοποίνου. Ειδικά ως προς την στοιχειοθέτηση τετελεσμένης χρήσης πλαστού μέσου πληρωμής γίνεται δεκτό ότι τετελεσμένη χρήση παραχαραγμένων νομισμάτων, με την έννοια της θέσης τους σε κυκλοφορία κατ' άρθρο 208 ΠΚ, υπάρχει μόνον τότε, όταν ο δράστης εξαπατά τον αποδέκτη τους παραπλανώντας τον ως προς τη γνησιότητα τους. Χωρίς αποδοχή του πλαστού μέσου πληρωμής, επομένως, μόνον απόπειρα του άρθρου 208 ΠΚ θα θεμελιώνεται. Η ολοκληρωμένη τέλεση χρήσης πλαστού εγγράφου δεν εξαρτάται αντιθέτως από την επιτυχία της εξαπάτησης. Η διαφοροποίηση αυτή των μέσων πληρωμής σε σχέση με τα υπομνήματα βασίζεται στην ιδιαίτερη λειτουργία τους, που ξεπερνώντας την αποδεικτική και εγγυητική των εγγράφων γίνεται συναλλακτική-εξοφλητική με την έννοια της διενέργειας πράξεων πληρωμής. Η πρόκληση περιουσιακής βλάβης θα ήταν επομένως

[124] Βλ. άρθρο 216 ΠΚ

[125] Βλ. άρθρο 208 ΠΚ

αναφαίρετη συνέπεια της θέσεως σε κυκλοφορία πλαστών μέσων πληρωμής κατά το άρθρο 208 ΠΚ.

Η ένταξη των «μέσων πληρωμής πλην των μετρητών» στο πεδίο ποινικής προστασίας του Θ' Κεφαλαίου του ΠΚ αποτελεί περαιτέρω συμμόρφωση με την ευρωπαϊκή επιταγή για εγκληματοποίηση τόσο των συνοδευτικών[126] όσο και των προπαρασκευαστικών[127] της πλαστοποίησης πράξεων.

Ανάγκη εναρμόνισης προκύπτει τέλος και ως προς την εγκληματοποίηση των προπαρασκευαστικών της απάτης με υπολογιστή πράξεων με την έννοια της κατασκευής, προμήθειας, κατοχής ή παραχώρησης προγραμμάτων υπολογιστή προορισμένων για την διάπραξη του εγκλήματος του άρθρου 386Α ΠΚ. Προτείνεται σχετικά η προσθήκη αντίστοιχης διάταξης στο άρθρο 386Α ΠΚ με πλαίσιο ποινής ελαφρώς χαμηλότερο από της καθαυτής απάτης.

Περαιτέρω, η ένταξη των «μέσων πληρωμής πλην των μετρητών» στο πεδίο εφαρμογής των άρθρων 207 και 208 ΠΚ θα διευκρλύνει την καταπολέμηση του σχετικού εγκληματικού φαινομένου εντάσσοντας το σε ένα ευρύτερο πλέγμα ποινικής θωράκισης κατά του οργανωμένου και οικονομικού εγκλήματος. Η συρροή των εγκλημάτων περί το νόμισμα (αλλά και του άρθρου 386Α ΠΚ) με το έγκλημα της σύστασης και ένταξης σε εγκληματική οργάνωση[128] ανοίγει νέες οδούς ποινικοδικονομικής δράσης με την ενεργοποίηση ειδικών ανακριτικών[129], ελεγκτικών και διωκτικών μηχανισμών[130].

---

[126] Βλ. άρθρο 207 ΠΚ περί κατοχής, προμήθειας, αποδοχής και μεταφοράς

[127] Βλ. άρθρο 211 ΠΚ

[128] Βλ. άρθρο 187 παρ. 1 ΠΚ

[129] Βλ. τις ειδικές ανακριτικές πράξεις του άρθρου Ζ53Α ΚΠΔ

[130] Βλ. άρθρο 2 παρ.2 περ. ια' ΠΔ 85/2005

## Επίλογος

Η τεχνολογία, οι ηλεκτρονικοί υπολογιστές και ο κυβερνοχώρος έχουν εισέλθει τα τελευταία χρόνια στην ζωή των ανθρώπων όλου, κυρίως του ανεπτυγμένου, κόσμου ενώ πλέον θα ήταν ουτοπικό να σκεφτόμαστε την καθημερινότητα χωρίς αυτά. Αναπόφευκτα η τεχνολογική έξαρση έχει δημιουργήσει έδαφος για νέες, ιδιόμορφες και εξεζητημένες απάτες, δίνοντας έτσι την δυνατότητα στους δράστες να διαπράττουν ποικίλα αδικήματα, που όπως είδαμε, αποφέρουν σε αυτούς τα επιθυμητά αποτελέσματα, δίνοντάς παράλληλα τη δυνατότητα να μην γίνεται ο εντοπισμός και η σύλληψη τους εύκολη για τις αρμόδιες αρχές.

Τα οικονομικό ηλεκτρονικό έγκλημα, το οποίο αποτελεί τις τελευταίες δεκαετίες μια από τις πιο εξελισσόμενες αλλά και απειλητικές για την κοινωνία, εκφάνσεις εγκλήματος αποφέρει στους δράστες του, άμεσα ή έμμεσα, τεράστια κεφάλαια ενώ οι ανεξέλεγκτες διαστάσεις που θεωρητικά μπορεί να λάβει το φαινόμενο αυτό στο εγγύς μέλλον προβληματίζουν έντονα την κοινή γνώμη αλλά και τις αρχές οι οποίες είναι επιφορτισμένες με την αντιμετώπισή του.

Στο ποινικό πεδίο οι έννομες τάξεις, σε όλα τα επίπεδα, έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικά τις διαμορφωμένες καταστάσεις, πιεζόμενες από τα πράγματα και τις εξελίξεις. Κλασσικό παράδειγμα είναι το θέμα που πραγματεύτηκε η παρούσα μελέτη, ο τομέας της τεχνολογίας και η εμφάνιση των οικονομικών εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές. Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και διαδικτύου. Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του εγκλήματος στον κυβερνοχώρο, χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Οι τεχνικές όμως γνώσεις δεν επαρκούν γα την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, για την κατανόηση των νομικών θεμάτων του διαδικτύου, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Οι Εισαγγελικές, Δικαστικές, Αστυνομικές κ.λ.π. αρχές δεν έχουν μέχρι στιγμής τις απαιτούμενες γνώσεις, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Και αυτό είναι πολύ λογικό, αφού ουδεμία εξειδικευμένη εκπαίδευση έχουν υποστεί μέχρι τώρα. Είναι βέβαιο δε ότι, εάν η Πολιτεία δε φροντίσει για την εκπαίδευσή τους στα αντίστοιχα θέματα, θα υπάρξει (στο πολύ σύντομο μέλλον) αδυναμία απονομής ορθής

## Πρωτογενείς πηγές

**Α. Διεθνείς Συμβάσεις**

Σύμβαση για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης, 23-11-2001 στη Βουδαπέστη

Committee on Payment and Settlement Systems (2003): A glossary of terms used in payments and settlement systems, March.

**Β. Ευρωπαϊκό δίκαιο**

**Οδηγίες – Συστάσεις - Αποφάσεις**

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά (ΕΕ L 178, 17.7.2000, σ. 1).

Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή

Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών

Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας

Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

Απόφαση-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών

Σχέδιο Δράσης με αριθμό 97/C 251/01για την καταπολέμηση του οργανωμένου εγκλήματος

Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών

Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν

στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων

Έκθεση της Επιτροπής που εκπονήθηκε κατ' εφαρμογή του άρθρου 14 της απόφασης-πλαισίου του Συμβουλίου της 28ης Μαΐου 2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών {SEC(2004) 532} /* COM/2004/0346 τελικό */

Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

Οδηγία 2007/64 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ και 2006/48/ΕΚ, και την κατάργηση της οδηγίας 97/5/ΕΚ

**Γ. <u>Νόμοι</u>**

Ποινικός κώδικας

Άρθρο 263α του Γερμανικού Ποινικού Κώδικα (263a StGB)

Ν.1805/1988 - «για εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές» *(ΦΕΚ* 199/Α΄/1988)

Ν.2246/1994 - «Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών» (ΦΕΚ/172/Α΄/20.10.1994)

Ν.2472/1997 - «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (*ΦΕΚ* 50/Α'/97)

Ν.2774/1999 - «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα» (ΦΕΚ 287/Α'/22.12.1999)

Ν.2867/2000 - «Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις» (*ΦΕΚ*/273/Α' /19.12.2000)

Ν. 2225/1994 (*ΦΕΚ* 121 Α΄/1994) όπως τροπ. με Ν. 3115/2003 - «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» (*ΦΕΚ* 47/Α/27.2.2003)

## Δευτερογενείς Πηγές

### Βιβλιογραφία - Αρθρογραφία

**Α. <u>Ελληνική</u>**

- **Αγγελής Ι. (2001),** Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), ΠοινΔικ 2001, σ. 1218 επ.
- **Αγγελής Ι.** «Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη» (http://www.lawnet.gr/pages/ eofn /2/cybercrime.asp)
- **Αγγελής Ι.,** Διαδίκτυο και ποινικό δίκαιο, Έγκλημα στον κυβερνοχώρο, Ποιν.Χρον Ν΄, 675 επ.
- **Αλεξανδρίδου Ε. (2004),** Το δίκαιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, σελ. 195 επ.
- **Ανδρουλάκης Ν. (1993),** Γύρω από την οικονομική εγκληματικότητα, Δ' Συνέδριο, Ελληνική Εταιρία Ποινικού Δικαίου, Τα οικονομικά εγκλήματα, Εκδόσεις Σάκκουλα, Αθήνα, σελ. 9.
- **Βασιλάκη Ε..** Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, σειρά ΠΟΙΝΙΚΑ, Νο 40, σελ. 133επ.
- **Βλαχόπουλος Κ. (2007),** Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη
- **Γιαννόπουλος Θ. (1986)** «Όψεις και Προβλήματα Ηλεκτρονικής Εγκληματικότητος», Νομική Βιβλιοθήκη, σελ. 170επ,
- **Γκόρτσος Βλ. Χρήστος. (2009),** Άρθρο, Η Οδηγία 2007/64/ΕΚ για τις υπηρεσίες πληρωμών στην εσωτερική αγορά -Συνολική θεώρηση, Οικονομική επιθεώρηση

- **Δούβλης Β. – Μπόλος Αγ. (2008)** Δίκαιο προστασίας καταναλωτών, Εκδ Σάκκουλα Αθήνα- Θεσσαλονίκη
- **Ζάννη Αν. (2005)** «Το διαδικτυακό έγκλημα», Εκδόσεις Σάκκουλα, Αθήνα
- **Ζησιάδης Β. (2001),** Η οικονομική εγκληματικότητα, το ουσιαστικό και δικονομικό οικονομικό Ποινικό Δίκαιο Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη
- **Καϊάφα- Γκμπάντι Μ. (2000),** «Το ποινικό δίκαιο στην καμπή του 2000: Με το βλέμμα προς το μέλλον χωρίς αποτίμηση του παρελθόντος;», Υπεράσπιση, σελ. 49-50,
- **Κωνσταντινίδης Α. (2000),** Η έννοια και λειτουργία του εγγράφου στο ουσιαστικό και δικονομικό ποινικό δίκαιο, σελ.117 επ
- **Κιούπης Δ. (1999),** Μονογραφιες, Ποινικό Δίκαιο και Internet, εκδόσεις Αντ. Σάκκουλα σελ. 145-176
- **Κονταξής Α. (2000)** Ποινικός Κώδικας Ερμηνεία κατ΄ άρθρο, Αθήνα.
- **Κουράκης Ν. (2005),** Το οικονομικό έγκλημα στην Ελλάδα σήμερα σε: του ιδίου Εγκληματολογικοί ορίζοντες Β΄, σελ. 163 επ., 183
- **Κουράκης, Ν. & Πατεράκης Ν. (2001)** «Το έγκλημα της απάτης», Νομική Βιβλιοθήκη, σελ. 209
- **Λάζος, Γ. (2001)** Πληροφορική & Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη
- **Μανωλεδάκης Ι., (1998)** Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου, Εκδόσεις. Σάκκουλα
- **Μυλωνόπουλος Χρ. (2000)** Ποινικό Δίκαιο Ειδικό Μέρος, εγκλήματα σχετικά με τα υπομνήματα εκδ. Σάκκουλα, σελ.8
- **Μυλωνόπουλος Χρ. (1991),** «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», Σειρά ΠΟΙΝΙΚΑ, Νο 33, , σελ. 14,
- **Ναμμίας Ο.**, Σύγχρονες μορφές απάτης στις τραπεζικές συναλλαγές Ένωση Ελλήνων Ποινικολόγων- Εθνική Τράπεζα της Ελλάδος Επιστημονική διημερίδα με θέμα Εγκλήματα στις τραπεζικές και χρηματιστηριακές συναλλαγές Αθήνα 18,19 Απριλίου 2003 . Επίσης σε Τιμητικό Τόμο Ν.Ανδρουλάκη σελ 467 επ. Εκδόσεις Α.Σάκκουλα 2003

- **Νούσκαλης Γ.**, Απάτη με Η/Υ το παρελθόν και το μέλλον του άρθρου 386Α Π.Κ ιδίως υπό το πρίσμα των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, Ποιν Δικ 2/2003, σελ 179
- **Πανούσης Ι. (1999),** Εγκληματολογία, Εγκληματολογική Έρευνα και ΜΜΕ, Εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή, σελ. 73
- **Στεφάνου, Κ.Α. – Χρ. Βλ. Γκόρτσος (2006):** *Διεθνές Οικονομικό Δίκαιο*, επικαιροποίηση του 11ου κεφαλαίου (Οκτ. 2009) σειρά μελετών Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, αρ. 1, Νομική Βιβλιοθήκη, Αθήνα
- **Συμεωνίδου – Καστανίδου Ελισάβετ (2006),** Για ένα νέο ορισμό του οργανωμένου εγκλήματος στην Ευρωπαϊκή Ένωση, Ποινικά Χρονικά 2006 (Ποιν. Χρον), σελ. 867
- **Τσαρούχας Κ.,** Η μαφία του διαδικτύου, Το Βήμα, 21 Ιουλίου 2002, σελ. Α34
- **Τσουραμάνης Χρήστος Ε (2005),** Ψηφιακή εγκληματικότητα, Η (αν)ασφαλής όψη του διαδικτύου . Εκδ. Κατσαρός, Αθήνα
- **Furnell, S. (2006)** Κυβερνοέγκλημα. Αθήνα: Παπαζήση.
- **R. Doswell & G. Simons (1990),** Πληροφορική και Εγκληματικότητα, Εκδόσεις Δαυλός, Αθήνα, σελ. 69 – 90
- **Sieber U.** Η εξέλιξη του Ποινικού Δικαίου στα πλαίσια της Ευρωπαϊκής Ένωσης Υπερ.4/1993.


**Β. <u>Ξενόγλωσση</u>**


- **Forester, Tom and Morrison, Perry (1994),** Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing. MIT Press
- **Anderson R. (2001)** «Security Engineering: A guide to building dependable distributed systems», New York: John Wiley and Sons, Inc
- **M. Collardin (1995),** Straftaeten im Internet, CR, σελ. 620, Schlmer/Conradi, Die Strafbarkeit der Internet Provider}, NStZ 1996, σελ. 369
- **A.M. Marshall & B.C. Tompsett, (2005)** Identity theft in an online world, Computer law & security report, 128 επ.

- **Geva, B. (2008):** TARGET2: Transfer of Funds and Harmonisation of EU Payment Law, *Uniform Commercial Code Law Journal*, vol. 41, No. 2, p. 113-123
- **Gercke (2005),** Die Strafbarkeit von " Phishing" und Identitätsdiebstahl, CR 2005, p.606
- **Eoghan,Casey (2004),** Digital Evidence and Computer Crime Εκδ. Elsevier Science & Technology
- **ECB (2009),** Glossary of terms related to payment, clearing and settlement systems, December


**Ηλεκτρονικές διευθύνσεις**


www.e-crime.gr/news.htm

http://www.pwc.com/gr/eng/ins-sol/spec-nt/pr_crime161007_GR.pdf

http://www.lawnet.gr/pages/eofn/2/cybercrime.asp

http://www.johnwasik.com/

http://de.wikipedia.org/wiki/Ulrich_Sieber

http://www.mekabay.com/

http://en.wikipedia.org/wiki/Phishing

http://en.wikipedia.org/wiki/Pharming

www.antiphishing.org

http://www.economicespionage.com/

http://en.wikipedia.org/wiki/Industrial_espionage

http://www.economicespionage.com/EEA.html

http://www.bankofgreece.gr/BoGDocuments/Καταστατικό_Έκδοση_Θ.pdf

http://www.ecb.de/pub/pdf/other/tagiel_bel.pdf

http://www.bankofgreece.gr/Pages/el/PaymentsSystems/largepayments.aspx

http://news.kathimerini.gr/4dcgi/_w_articles_economy_1_27/06/2009_320084

http://www.go-online.gr/ebusiness/specials/article.html

http://www.nb.org/?pgtp=31&pId=744

http://www.go-online.gr/ebusiness/specials/article.html?article_id=368

http://www.bis.org/publ/cpss22.htm

http://www.bankofgreece.gr/Pages/el/PaymentsSystems/default.aspx

http://www.bankofgreece.gr/Pages/el/PaymentsSystems/oversight.aspx

http://www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=90

http://www.hcba.gr/?pgtp=1&aid=25

http://www.bis.org/cpss/index.htm